ID: 830321
Sample Name: click.wsf
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 09:06:00
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

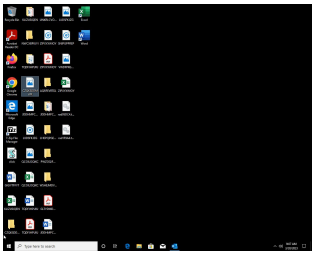
Windows Analysis Report

click.wsf

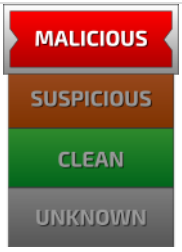
Overview

General Information

Sample Name:	click.wsf
Analysis ID:	830321
MD5:	016fa961b9af4…
SHA1:	2fee0634cfa29…
SHA256:	8343af0017ad6..
Infos:	



Detection



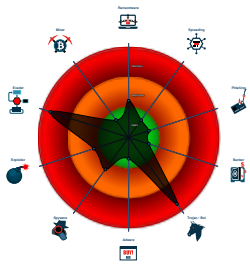
Emotet

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

Signatures

- Benign windows process drops PE f…
- VBScript performs obfuscated calls…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Run temp file via re…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 804 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- wscript.exe (PID: 6404 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\click.wsf" MD5: 563EDAE37876138FDFF47F3E7A9A78FD)
  - regsvr32.exe (PID: 6508 cmdline: C:\Windows\System32\regsvr32.exe "C:\Users\user\Desktop\rad75349.tmp.dll MD5: 578BAB56836A3FE455FFC7883041825B)
    - regsvr32.exe (PID: 6544 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\BlUwZJEPejvMeG\xhwdmo.dll" MD5: 578BAB56836A3FE455FFC7883041825B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Emotet	While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets.It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time.Emotet had been taken down by authorities in January 2021, though it appears to have sprung back to life in November 2021.	• GOLD CABIN • MUMMY SPIDER • Mealybug	http://blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/http://ropgadget.com/posts/defensive_pcres.htmlhttps://adalogics.com/blog/the-state-of-advanced-code-injectionshttps://asec.ahnlab.com/en/33600/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "91.121.146.47:8080",
    "66.228.32.31:7080",
    "182.162.143.56:443",
    "187.63.160.88:80",
    "167.172.199.165:8080",
    "164.90.222.65:443",
    "104.168.155.143:8080",
    "163.44.196.120:8080",
    "160.16.142.56:8080",
    "159.89.202.34:443",
    "159.65.88.10:8080",
    "186.194.240.217:443",
    "149.56.131.28:8080",
    "72.15.201.15:8080",
    "1.234.2.232:8080",
    "82.223.21.224:8080",
    "206.189.28.199:8080",
    "169.57.156.166:8080",
    "107.170.39.149:8080",
    "103.43.75.120:443",
    "91.207.28.33:8080",
    "213.239.212.5:443",
    "45.235.8.30:8080",
    "119.59.103.152:8080",
    "164.68.99.3:8080",
    "95.217.221.146:8080",
    "153.126.146.25:7080",
    "197.242.150.244:8080",
    "202.129.205.3:8080",
    "103.132.242.26:8080",
    "139.59.126.41:443",
    "110.232.117.186:8080",
    "183.111.227.137:8080",
    "5.135.159.50:443",
    "201.94.166.162:443",
    "103.75.201.2:443",
    "79.137.35.198:8080",
    "172.105.226.75:8080",
    "94.23.45.86:4143",
    "115.68.227.76:8080",
    "153.92.5.27:8080",
    "167.172.253.162:8080",
    "188.44.20.25:443",
    "147.139.166.154:8080",
    "129.232.188.93:443",
    "173.212.193.249:8080",
    "185.4.135.165:8080",
    "45.176.232.124:443"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5MHq6bwAsAIA=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2snoEbwASAJI="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.1414548751.000002D845C7D000.00000004.00000020.00020000.00000000.sdmp	webshell_asp_obfuscated	ASP webshell obfuscated	Arnim Rupp	• 0x80c:$tagasp_long20: <script language="VB • 0x79f:$asp_payload9: execute " • 0xb2:$m_multi_one4: mid(• 0x2fb:$m_multi_one4: mid(• 0x4c8:$m_multi_one4: mid(• 0x6d1:$m_multi_one4: mid(• 0xa4c:$m_multi_one4: mid(

Source	Rule	Description	Author	Strings
00000001.00000002.1552503322.000002D84653C000.00000004.00000020.00020000.00000000.sdmp	WEBSHELL_asp_generic	Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file	Arnim Rupp	• 0x312:$asp_gen_obf1: "+" • 0x342:$asp_gen_obf1: "+" • 0x1bd6:$tagasp_classid5: 0D43FE01-F093-11CF-8940-00A0C9054228 • 0x7a6:$jsp4: public • 0xde6:$jsp4: public • 0x126:$asp_input1: request • 0x954:$asp_input1: request • 0x996:$asp_input1: request • 0xaac:$asp_input1: request • 0x1e96:$asp_input1: request • 0x460:$asp_payload11: wscript.shell • 0x48:$asp_multi_payload_one1: createobject • 0x136:$asp_multi_payload_one1: createobject • 0x1ae:$asp_multi_payload_one1: createobject • 0x208:$asp_multi_payload_one1: createobject • 0x444:$asp_multi_payload_one1: createobject • 0xbaa:$asp_multi_payload_one1: createobject • 0xee2:$asp_multi_payload_one1: createobject • 0x1db8:$asp_multi_payload_one1: createobject • 0x1ea6:$asp_multi_payload_one1: createobject • 0x1f1e:$asp_multi_payload_one1: createobject
00000001.00000003.1530447488.000002D846461000.00000004.00000020.00020000.00000000.sdmp	webshell_asp_obfuscated	ASP webshell obfuscated	Arnim Rupp	• 0xdea6:$tagasp_classid1: 72C24DD5-D70A-438B-8A42-98424B88AFB8 • 0x1726:$jsp4: public • 0x1d66:$jsp4: public • 0x9726:$jsp4: public • 0x9d66:$jsp4: public • 0xb736:$jsp4: public • 0xbd76:$jsp4: public • 0xc786:$jsp4: public • 0xcdc6:$jsp4: public • 0x13e0:$asp_payload11: wscript.shell • 0x93e0:$asp_payload11: wscript.shell • 0xb3f0:$asp_payload11: wscript.shell • 0xc440:$asp_payload11: wscript.shell • 0xfc8:$asp_multi_payload_one1: createobject • 0x10b6:$asp_multi_payload_one1: createobject • 0x112e:$asp_multi_payload_one1: createobject • 0x1188:$asp_multi_payload_one1: createobject • 0x13c4:$asp_multi_payload_one1: createobject • 0x1b2a:$asp_multi_payload_one1: createobject • 0x1e62:$asp_multi_payload_one1: createobject • 0x8fc8:$asp_multi_payload_one1: createobject
00000001.00000003.1530447488.000002D846461000.00000004.00000020.00020000.00000000.sdmp	WEBSHELL_asp_generic	Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file	Arnim Rupp	• 0x1292:$asp_gen_obf1: "+" • 0x12c2:$asp_gen_obf1: "+" • 0x9292:$asp_gen_obf1: "+" • 0x92c2:$asp_gen_obf1: "+" • 0xb2a2:$asp_gen_obf1: "+" • 0xb2d2:$asp_gen_obf1: "+" • 0xc2f2:$asp_gen_obf1: "+" • 0xc322:$asp_gen_obf1: "+" • 0xdea6:$tagasp_classid1: 72C24DD5-D70A-438B-8A42-98424B88AFB8 • 0x1726:$jsp4: public • 0x1d66:$jsp4: public • 0x9726:$jsp4: public • 0x9d66:$jsp4: public • 0xb736:$jsp4: public • 0xbd76:$jsp4: public • 0xc786:$jsp4: public • 0xcdc6:$jsp4: public • 0x10a6:$asp_input1: request • 0x18d4:$asp_input1: request • 0x1916:$asp_input1: request • 0x1a2c:$asp_input1: request
00000003.00000002.1502600709.0000000000731000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.regsvr32.exe.460000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.460000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Sigma Signatures

Malware Analysis System Evasion

Sigma detected: Run temp file via regsvr32

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 8 - Source IP: 192.168.2.3 - Destination IP: 187.63.160.88

Timestamp:	192.168.2.3187.63.160.8849735802404314 03/20/23-09:07:57.133517
SID:	2404314
Source Port:	49735
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 7 - Source IP: 192.168.2.3 - Destination IP: 182.162.143.56

Timestamp:	192.168.2.3182.162.143.56497344432404312 03/20/23-09:07:41.132019
SID:	2404312
Source Port:	49734
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 2 - Source IP: 192.168.2.3 - Destination IP: 104.168.155.143

Timestamp:	192.168.2.3104.168.155.1434973880802404302 03/20/23-09:08:15.086032
SID:	2404302
Source Port:	49738
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 23 - Source IP: 192.168.2.3 - Destination IP: 91.121.146.47

Timestamp:	192.168.2.391.121.146.474973180802404344 03/20/23-09:07:19.650620
SID:	2404344
Source Port:	49731
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 5 - Source IP: 192.168.2.3 - Destination IP: 164.90.222.65

Timestamp:	192.168.2.3164.90.222.65497374432404308 03/20/23-09:08:10.886539
SID:	2404308
Source Port:	49737
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 6 - Source IP: 192.168.2.3 - Destination IP: 167.172.199.165

Timestamp:	192.168.2.3167.172.199.1654973680802404310 03/20/23-09:08:05.635641
SID:	2404310
Source Port:	49736
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 16 - Source IP: 192.168.2.3 - Destination IP: 66.228.32.31

Timestamp:	192.168.2.366.228.32.314973370802404330 03/20/23-09:07:25.133944
SID:	2404330
Source Port:	49733
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

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

Benign windows process drops PE files

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

Stealing of Sensitive Information

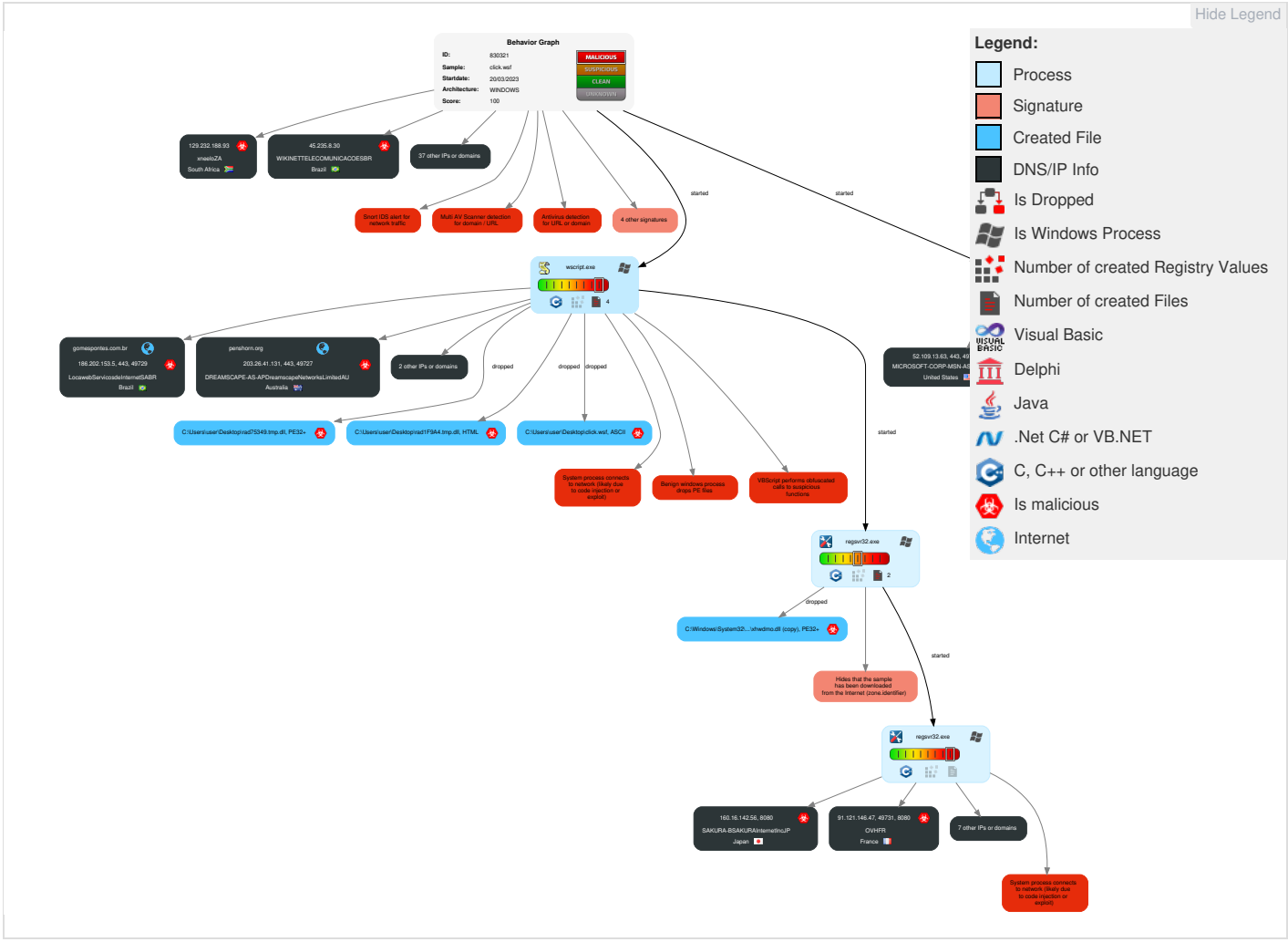
Yara detected Emotet

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	1 2 Scripting	1 DLL Side-Loading	1 1 1 Process Injection	2 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	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 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Scripting	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Non-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 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 5 Application Layer Protocol	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 4 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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	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

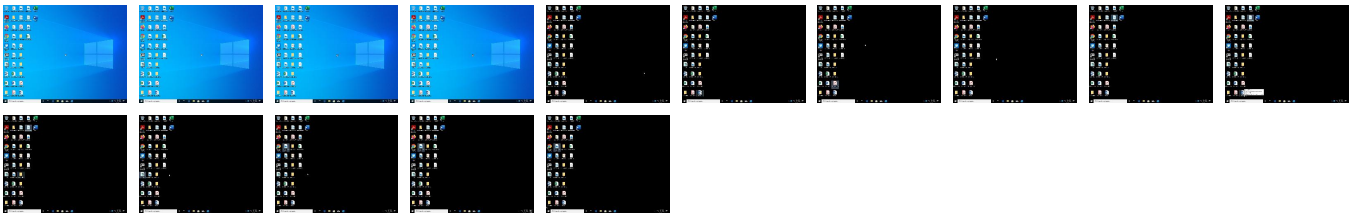
Behavior Graph

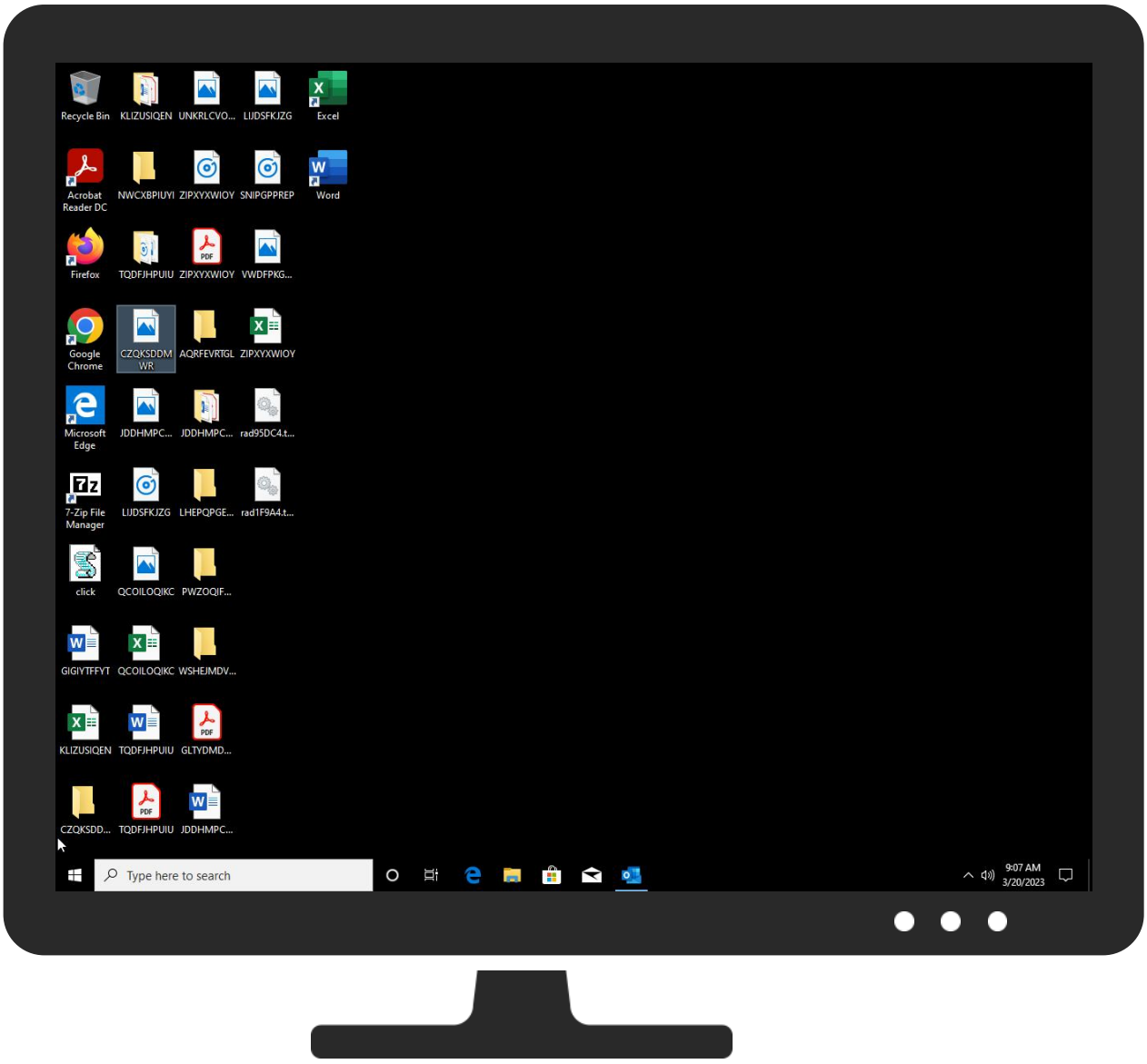


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\rad75349.tmp.dll	79%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\BlUwZJEPejvMeG\xhwdmo.dll (copy)	79%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.regsvr32.exe.460000.0.unpack	100%	Avira	HEUR/AGEN.1215476		Download File

Domains

Source	Detection	Scanner	Label	Link
bbvoyage.com	9%	Virustotal		Browse
gomespontes.com.br	2%	Virustotal		Browse
penshorn.org	14%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.gomespontes.com.br	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://softwareulike.com/cWIYxWMPkK/	100%	Avira URL Cloud	malware	
http://wrappixels.co	0%	Avira URL Cloud	safe	
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/H#K#0	100%	Avira URL Cloud	malware	
http://https://160.16.142.56:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	0%	Avira URL Cloud	safe	
http://https://160.16.142.56:8080/M	0%	Avira URL Cloud	safe	
http://https://187.63.160.88:80/wfqhlvcfruxkwghn/ivirkxueekmcz/VnX	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/wfqhlvcfruxkwghn/ivirkxueekmcz/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/X	100%	Avira URL Cloud	malware	
http://https://bbvoyage.com/useragreement/ElKHvb4QIQqSrh6Hqm/	100%	Avira URL Cloud	malware	
http://https://163.44.196.120:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/bK	100%	Avira URL Cloud	malware	
http://https://104.168.155.143:8080/Y	100%	Avira URL Cloud	malware	
http://https://163.44.196.120:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/z	100%	Avira URL Cloud	malware	
http://https://163.44.196.120:8080/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/logs/pd/vM	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/l	100%	Avira URL Cloud	malware	
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/cw34006	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/dllgz	100%	Avira URL Cloud	malware	
http://https://187.63.160.88:80/wfqhlvcfruxkwghn/ivirkxueekmcz/	100%	Avira URL Cloud	malware	
http://https://163.44.196.120:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/s	0%	Avira URL Cloud	safe	
http://ozmeydan.com/cekici/9/	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/)	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/logs/pd/	100%	Avira URL Cloud	malware	
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/wM	100%	Avira URL Cloud	malware	
http://https://160.16.142.56:8080/wfqhlvcfruxkwghn/ivirkxueekmcz//	0%	Avira URL Cloud	safe	
http://https://penshorn.org/admin/Ses8712iGR8du/tM	100%	Avira URL Cloud	malware	
http://https://104.168.155.143:8080/4	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/	0%	Avira URL Cloud	safe	
http://https://164.90.222.65/wfqhlvcfruxkwghn/ivirkxueekmcz/	100%	Avira URL Cloud	malware	
http://https://bbvoyage.com/useragreement/ElKHvb4QIQqSrh6Hqm/uM	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	100%	Avira URL Cloud	malware	
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/	100%	Avira URL Cloud	malware	
http://https://penshorn.org/admin/Ses8712iGR8du/	100%	Avira URL Cloud	malware	
http://softwareulike.com/cWIYxWMPkK/yM	100%	Avira URL Cloud	malware	
http://https://104.168.155.143:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/wfqhlvcfruxkwghn/ivirkxueekmcz/.DLL	100%	Avira URL Cloud	malware	
http://ozmeydan.com/cekici/9/xM	100%	Avira URL Cloud	malware	
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/dll	100%	Avira URL Cloud	malware	
http://https://104.168.155.143:8080/P	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/logs/pd/l	100%	Avira URL Cloud	malware	
http://https://104.168.155.143:8080/	100%	Avira URL Cloud	malware	
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/	100%	Avira URL Cloud	malware	
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/zM	100%	Avira URL Cloud	malware	
http://https://160.16.142.56:8080/	0%	Avira URL Cloud	safe	
http://https://91.121.146.47:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	100%	Avira URL Cloud	malware	
http://https://penshorn.org/admin/Ses8712iGR8du/95DC4.tmp.dll(	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/logs/pd/0w	100%	Avira URL Cloud	malware	
http://softwareulike.com/cWIYxWMPkK/_	100%	Avira URL Cloud	malware	
http://https://160.16.142.56:8080/)	0%	Avira URL Cloud	safe	
http://https://bbvoyage.com/useragreement/ElKHvb4QIQqSrh6Hqm/476	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bbvoyage.com	31.31.196.172	true	true	• 9%, Virustotal, Browse	unknown
gomespontes.com.br	186.202.153.5	true	true	• 2%, Virustotal, Browse	unknown
penshorn.org	203.26.41.131	true	true	• 14%, Virustotal, Browse	unknown
www.gomespontes.com.br	unknown	unknown	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bbvoyage.com/useragreement/ElKHvb4QIQqSrh6Hqm/	true	• Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/logs/pd/	true	• Avira URL Cloud: malware	unknown
http://https://164.90.222.65/wfqhlvcfruxkwghn/ivirkxueekmcz/	true	• Avira URL Cloud: malware	unknown
http://https://penshorn.org/admin/Ses8712iGR8du/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/H#K#0	wscript.exe, 00000001.00000003.141730125 4.000002D845C83000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://wrappixels.co	wscript.exe, 00000001.00000003.154274177 8.000002D845C90000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://softwareulike.com/cWIYxWMPkK/	wscript.exe, wscript.exe, 00000001.00000003.152940 4109.000002D8463EE000.00000004.00000020. 00020000.00000000.sdmp, wscript.exe, 000 00001.00000003.1521966849.000002D84626F0 00.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000 002D846412000.00000004.00000020.00020000 .00000000.sdmp, wscript.exe, 00000001.00 000003.1505842083.000002D845E4E000.00000 004.00000020.00020000.00000000.sdmp, wsc ript.exe, 00000001.00000003.1526888779.0 00002D8462D5000.00000004.00000020.000200 00.00000000.sdmp, wscript.exe, 00000001. 00000003.1526294634.000002D84631A000.000 00004.00000020.00020000.00000000.sdmp, w script.exe, 00000001.00000003.1528804146 .000002D8462B3000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000002.1552503322.000002D84653C000.0 0000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.15304474 88.000002D846461000.00000004.00000020.00 020000.00000000.sdmp, wscript.exe, 00000 001.00000003.1509441394.000002D845E4A000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507610198.00000 2D845DF6000.00000004.00000020.00020000.0 0000000.sdmp, wscript.exe, 00000001.0000 0003.1507946268.000002D845ED2000.0000000 4.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000002D8463EE 000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1504930637.00 0002D8466C5000.00000004.00000020.0002000 0.00000000.sdmp, wscript.exe, 00000001.0 0000003.1514390296.000002D84600D000.0000 0004.00000020.00020000.00000000.sdmp, ws cript.exe, 00000001.00000003.1507946268. 000002D845EB1000.00000004.00000020.00020 000.00000000.sdmp, wscript.exe, 00000001 .00000003.1511499007.000002D845F4D000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.152749202 7.000002D846291000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 01.00000003.1519488621.000002D846065000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002 D845E94000.00000004.00000020.00020000.00 000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://160.16.142.56:8080/M	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D51000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://160.16.142.56:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000002.2661608245.0000000000D6800 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://187.63.160.88:80/wfqhlvcfruxkwghn/ivirkxueekmcz/VnX	regsvr32.exe, 00000004.00000003.23673423 15.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://66.228.32.31:7080/wfqhlvcfruxkwghn/ivirkxueekmcz/	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000003.2367342315.0000000000D5800 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://91.121.146.47:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/X	regsvr32.exe, 00000004.00000003.18684385 31.0000000000D08000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://104.168.155.143:8080/Y	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://163.44.196.120:8080/wfqhlvcfruxkwghn/ivirkxuekmcz/bK	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://91.121.146.47:8080/	regsvr32.exe, 00000004.00000002.26616082 45.0000000000CFB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000003.2367342315.0000000000CF600 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000003.1868438531.000 0000000CE0000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://163.44.196.120:8080/	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://163.44.196.120:8080/wfqhlvcfruxkwghn/ivirkxuekmcz/z	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D51000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/logs/pd/vM	wscript.exe, 00000001.00000003.141722746 8.000002D845C90000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 01.00000003.1542741778.000002D845C90000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/cw34006	wscript.exe, 00000001.00000003.153199278 0.000002D8464BA000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 01.00000002.1552238532.000002D8464BB000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/l	regsvr32.exe, 00000004.00000003.23673423 15.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000003.2367342315.0000000000D5800 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://91.121.146.47:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/dllgz	regsvr32.exe, 00000004.00000002.26609860 60.0000000000C99000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://187.63.160.88:80/wfqhlvcfruxkwghn/ivirkxueekmcz/	regsvr32.exe, 00000004.00000003.23673423 15.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://163.44.196.120:8080/wfqhlvcfruxkwghn/ivirkxuekmcz/	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D58000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/s	wscript.exe, 00000001.00000002.155471080 7.000002D846747000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

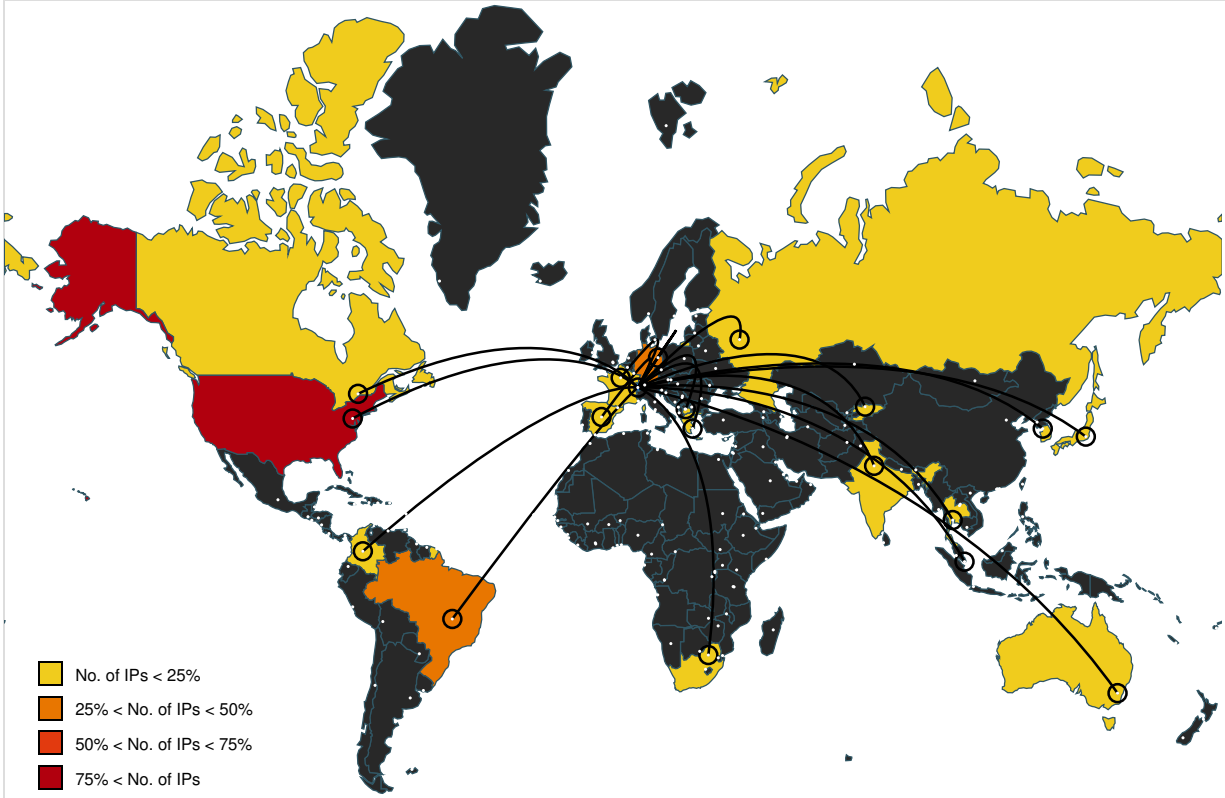
Name	Source	Malicious	Antivirus Detection	Reputation
http://ozmeydan.com/cekici/9/	wscript.exe, wscript.exe, 00000001.00000003.1529404109.000002D8463EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1521966849.000002D84626F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000002D846412000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1505842083.000002D845E4E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1526888779.000002D8462D5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1526294634.000002D84631A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1528804146.000002D8462B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.1552503322.000002D84653C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1530447488.000002D846461000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1509441394.000002D845E4A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507610198.000002D845DF6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845ED2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000002D8463EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1504930637.000002D8466C5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.1553706057.000002D8466F1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1514390296.000002D84600D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845EB1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1511499007.000002D845F4D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1527492027.000002D846291000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1519488621.000002D846065000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://164.90.222.65/)	regsvr32.exe, 00000004.00000003.2367342315.0000000000D51000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/wM	wscript.exe, 00000001.00000003.1417227468.000002D845C90000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1542741778.000002D845C90000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://160.16.142.56:8080/wfqhlvcfruxkwghn/ivirkxueekmcz//	regsvr32.exe, 00000004.00000002.2661608245.0000000000D58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://penshorn.org/admin/Ses8712iGR8du/tM	wscript.exe, 00000001.00000003.1417227468.000002D845C90000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1542741778.000002D845C90000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://104.168.155.143:8080/4	regsvr32.exe, 00000004.00000002.2661608245.0000000000D58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/	wscript.exe, 00000001.00000003.1537553114.000002D84656F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1542696917.000002D846570000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1540601110.000002D846570000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1534710579.000002D846568000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1545756551.000002D846570000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bbvoyage.com/useragreement/ElKHvb4QIQqSrh6Hqm/uM	wscript.exe, 00000001.00000003.1417227468.000002D845C90000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1542741778.000002D845C90000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://66.228.32.31:7080/wfqhlvcfruxkwghn/ivirkxueekmcz/.DLL	regsvr32.exe, 00000004.00000002.2661608245.0000000000D58000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000003.2367342315.0000000000D58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/	wscript.exe, wscript.exe, 00000001.00000003.1529404109.000002D8463EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1521966849.000002D84626F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000002D846412000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1505842083.000002D845E4E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1526888779.000002D8462D5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1526294634.000002D84631A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1528804146.000002D8462B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.1552503322.000002D84653C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1530447488.000002D846461000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1509441394.000002D845E4A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507610198.000002D845DF6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845ED2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000002D8463EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1504930637.000002D8466C5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1514390296.000002D84600D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845EB1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1511499007.000002D845F4D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1527492027.000002D846291000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1519488621.000002D846065000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845E94000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://softwareulike.com/cWIYxWMPkK/yM	wscript.exe, 00000001.00000003.1417227468.000002D845C90000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1542741778.000002D845C90000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	regsvr32.exe, 00000004.00000003.2367342315.0000000000D58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://104.168.155.143:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	regsvr32.exe, 00000004.00000002.2661608245.0000000000CD4000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000002.2661608245.0000000000CEB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/dll	wscript.exe, 00000001.00000002.1551840814.000002D84606B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1514223112.000002D84605E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://ozmeydan.com/cekici/9/xM	wscript.exe, 00000001.00000003.1417227468.000002D845C90000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1542741778.000002D845C90000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://104.168.155.143:8080/P	regsvr32.exe, 00000004.00000002.2661608245.0000000000D58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/logs/pd/l	wscript.exe, 00000001.00000002.1551840814.000002D84606B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1514223112.000002D84605E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://104.168.155.143:8080/	regsvr32.exe, 00000004.00000002.2661608245.0000000000D58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/	wscript.exe, wscript.exe, 00000001.00000003.1529404109.000002D8463EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1521966849.000002D84626F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000002D846412000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1505842083.000002D845E4E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1526888779.000002D8462D5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1526294634.000002D84631A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1528804146.000002D8462B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.1552503322.000002D84653C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1530447488.000002D846461000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1509441394.000002D845E4A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507610198.000002D845DF6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845ED2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1548494229.000002D8463EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1504930637.000002D8466C5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1514390296.000002D84600D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845EB1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1511499007.000002D845F4D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1527492027.000002D846291000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1519488621.000002D846065000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1507946268.000002D845E94000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/zM	wscript.exe, 00000001.00000003.1417227468.000002D845C90000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://160.16.142.56:8080/	regsvr32.exe, 00000004.00000002.2661608245.0000000000D6A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000004.00000002.2661608245.0000000000D51000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://91.121.146.47:8080/wfqhlvcfruxkwghn/ivirkxueekmcz/	regsvr32.exe, 00000004.00000002.2660986060.0000000000C99000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://penshorn.org/admin/Ses8712iGR8du/95DC4.tmp.dll(	wscript.exe, 00000001.00000002.1551840814.000002D84606B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.1514223112.000002D84605E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/logs/pd/0w	wscript.exe, 00000001.00000003.1541349732.000002D846702000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.1553706057.000002D84672F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://softwareulike.com/cWIYxWMPkK/_	wscript.exe, 00000001.00000003.141730125 4.000002D845C83000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://160.16.142.56:8080/)	regsvr32.exe, 00000004.00000002.26616082 45.0000000000D51000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://bbvoyage.com/useragreement/ElKHvb4QIQqSr h6Hqm/476	wscript.exe, 00000001.00000003.153199278 0.000002D8464BA000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 01.00000002.1552238532.000002D8464BB000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.109.13.63	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
103.132.242.26	unknown	India		45117	INPL-IN-APIshansNetworkIN	true
104.168.155.143	unknown	United States		54290	HOSTWINDSUS	true
79.137.35.198	unknown	France		16276	OVHFR	true
115.68.227.76	unknown	Korea Republic of		38700	SMILESERV-AS-KRSMILESERVKR	true
163.44.196.120	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
206.189.28.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
31.31.196.172	bbvoyage.com	Russian Federation		197695	AS-REGRU	true
186.202.153.5	gomespontes.com.br	Brazil		27715	LocawebServicosdeInternetSABR	true
203.26.41.131	penshorn.org	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
107.170.39.149	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
66.228.32.31	unknown	United States		63949	LINODE-APLinodeLLCUS	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
185.4.135.165	unknown	Greece		199246	TOPHOSTGR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
183.111.227.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
169.57.156.166	unknown	United States		36351	SOFTLAYERUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
139.59.126.41	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
167.172.199.165	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
202.129.205.3	unknown	Thailand		45328	NIPA-AS-THNIPATECHNOLOGYCOLTDTH	true
147.139.166.154	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
153.92.5.27	unknown	Germany		47583	AS-HOSTINGERLT	true
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.226.75	unknown	United States		63949	LINODE-APLinodeLLCUS	true
164.90.222.65	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
213.239.212.5	unknown	Germany		24940	HETZNER-ASDE	true
5.135.159.50	unknown	France		16276	OVHFR	true
186.194.240.217	unknown	Brazil		262733	NetceteraTelecomunicacoesLtdaBR	true
119.59.103.152	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
159.89.202.34	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
91.121.146.47	unknown	France		16276	OVHFR	true
160.16.142.56	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
91.207.28.33	unknown	Kyrgyzstan		39819	PROHOSTKG	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
103.43.75.120	unknown	Japan		20473	AS-CHOOPAUS	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
45.235.8.30	unknown	Brazil		267405	WIKINETTELECOMUNICACOESBR	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
187.63.160.88	unknown	Brazil		28169	BITCOMPROVEDORDESERVICOSDEINTERNETLTDABR	true
82.223.21.224	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
95.217.221.146	unknown	Germany		24940	HETZNER-ASDE	true
149.56.131.28	unknown	Canada		16276	OVHFR	true
182.162.143.56	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
52.109.76.141	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
94.23.45.86	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830321

Start date and time:	2023-03-20 09:06:00 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
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
Sample file name:	click.wsf
Detection:	MAL
Classification:	mal100.troj.evad.winWSF@5/8@3/54
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 50.2% (good quality ratio 42.4%) • Quality average: 60.5% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .wsf

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 8.253.95.121, 8.241.121.126, 8.241.123.126, 8.248.135.254, 67.27.234.126
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, login.live.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:06:48	API Interceptor	2x Sleep call for process: wscript.exe modified
09:07:20	API Interceptor	8x Sleep call for process: regsvr32.exe modified

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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62582 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62582
Entropy (8bit):	**7.996063107774368**
Encrypted:	**true**
SSDEEP:	1536:Jk3XPi43VgGp0gB2itudTSRAn/TWTdWftu:CHa43V5p022iZ4CgA
MD5:	E71C8443AE0BC2E282C73FAEAD0A6DD3
SHA1:	0C110C1B01E68EDFACAEAE64781A37B1995FA94B
SHA-256:	95B0A5ACC5BF70D3ABDFD091D0C9F9063AA4FDE65BD34DBF16786082E1992E72
SHA-512:	B38458C7FA2825AFB72794F374827403D5946B1132E136A0CE075DFD351277CF7D957C88DC8A1E4ADC3BCAE1FA8010DAE3831E268E910D517691DE24326391A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....v.....,.....I.....BVrl .authroot.stl....oJ5..CK..8U....a..3.1.P. J."..t..2F2e.dHH.....$E.KB.2D..-SJE....^..'..y.}...,{m.....\...]4.G.....h....148...e.gr.....48:.L. ..g.....Xef.x:..t...J...6-....kW6Z>....&.....ye.U.Q&z:.vZ..._....a...]..T.E.....B.h.,...[....V.O.3..EW.x.?.Q..$.@.W..=.B.f..8a.Y.JK..g./%p..C.4CD.s..Jd.u..@.g=...a.. .h%..'.xjy7.E ..\.....A..':.4TdW?Ko3$.Hg.z.d~...../q..C.....`...A[ W(.....9...GZ.;....I&?.....F...p?... .p.....{S.L4..v.+...7.T?.....p..`..&..9.....f...0+.L.....1.2b)..vX5L'.~....2vz.,E.Ni.{#...o..w.?.#.3 ..h.v<.S%.].tD@!Le.w.q.7.8....QW.FT.....hE.....Y...../.%Q...k...*.Y.n..v.A..../...>B..5\..-Ko.....O<.b.K.{.O.b...._.7...4.;%9N..K.X>.....kg-9..r.c.g.G|.*[.-...HT...",?.q...ad. ...7RE.....!f..#../....?.-.^.K.c^...+{.g.....]<..$.=.O....ii7.wJ+S..Z..d.....>..J*...T..Q7..`.r,<$....\d:K`..T.n....N.....C..j.;.1SX..j....1...R....+....Yg....]....3..9..S..D..`.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.127437612314223
Encrypted:	false
SSDEEP:	6:kKnMAry/7UN+SkQlPlEGYRMY9z+4KlDA3RUecZUt:PMoCvkPlE99SNxAhUext
MD5:	DB2EC1D25EBBF63A67B76A991DE9381B
SHA1:	ED66F35D9308016B4F276CC09C3B2116669070E5
SHA-256:	E7E343FE929301E443F44F2842348A4875C87ABD0CF3B2F29403C96A660344AA
SHA-512:	03D7D4AE006B25E50EA4F98ADD852997D7E11A6064AE0334A2BA0D0056E15F5C432990EDC79FA4C00F57A0A44C71982DC302636E17F46A95CAE85814AF7400FC
Malicious:	false
Preview:	p..... .....Z.L..[..(..... .....).K.....&.....v...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.2.f.9.2.9.a.7.4.b.d.9.1.:.0."...

C:\Users\user\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230320T0906180748-804.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	old-fs dump file (16-bit, assuming PDP-11 endianness), Previous dump Thu Jan 1 01:07:36 1970, This dump Thu Jan 1 01:09:04 1970,
Category:	modified
Size (bytes):	8192
Entropy (8bit):	4.3056677894243895
Encrypted:	false
SSDEEP:	48:oG+4F4x8t4OU4oxJN4rXVJVpV+VuVSV1y8wfZu+E+d2nYgFxvZPEGsj6xYw6vMI:TU8c9dK2nrFrTCMI
MD5:	8A4B17DA69383C75316D7488A1F36DEB

SHA1:	04AA89B2ECD1EA38D81AD9865450CF02F9A709C5
SHA-256:	882EE2DE3174D9BA48B2B58B5ACEA99F69EB8D5594F7ED2DD5C6C7FA47B71B2A
SHA-512:	E397B0E0D7701583A8E2CCD097E78A881C826B7DC0696595107657DEDEF826FAED3D522C80605ED83B7119081667DA58730A65BFE6828C25BF7E02404AD8A65
Malicious:	false
Preview:	........0....._k..[..&..... ...h.1.<...8 .~<...X.....$.....?..[..#..*...C.L...0T.j.....B.....[.X.....$.....?..[..#..*...C.L...0T.j.....[...B..... .....f.`.....$.....?..[..#..*...C.L...0T.i.....&..B.....$.....?..[..0.K(.J.J.C.....@..... ..B.....M.i.c.r.o.s.o.f.t...O.f.f.i.c.e. ..O.u.t.l.o.o.k...C.l.o.u.d.S.e.t.t.i.n.g.s...D.e.f.a.u.l.t.E.n.a.b.l.e.d.S.t.a.t.u.s...].....0.0.....$.....?..[..0.K(.J.J.C.....@.....1.B.....M.i.c.r.o.s.o.f.t...O.f.f. i.c.e...O.u.t.l.o.o.k...R.i.p.C.o.r.d...4.7.2.6.4.2.8.....0.P.....$....HF..[....{(.Z/K.i.a..ZIs.....9.B.....P.....$....HF..[....{(.Z/K.i.a..ZIt.....F.B..... .....P.....$....HF..[....{(.Z/K.i.a..ZIs.....M.B.....P.....$....HF..[..

C:\Users\user\Desktop\click.wsf

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	9
Entropy (8bit):	2.94770277922009
Encrypted:	false
SSDEEP:	3:tWn:tWn
MD5:	07F5A0CFFD9B2616EA44FB90CCC04480
SHA1:	641B12C5FFA1A31BC367390E34D441A9CE1958EE
SHA-256:	A0430A038E7D879375C9CA5BF94CB440A3B9A002712118A7BCCC1FF82F1EA896
SHA-512:	09E7488C138DEAD45343A79AD0CB37036C5444606CDFD8AA859EE70227A96964376A17F07E03D0FC353708CA9AAF979ABF8BC917E6C2D005A0052575E074F53
Malicious:	**true**
Preview:	badum tss

C:\Users\user\Desktop\rad1F9A4.tmp.dll

Process:	C:\Windows\System32\wscript.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.035593451835013
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwq8B0hEr6VHB0SpMAcg/EzBoAuZ2A3b1AYDAJgXPUhA1QCV2AmWZW5Kk:J0+oxb8ShRZSS146Ai2A3JAhSPEAr1mP
MD5:	118A489422BE0C5CA0CECF3BB7903C7E
SHA1:	B90AF089FD0E728E61D532BE80062AED39D98978
SHA-256:	FF6D14F77E27F7B90CB2F20BCE408189F5F388961F3FCD13FE2DF2CC0A002DC3
SHA-512:	283CD22F52BCCB8DD22A8772E8121302A6975F2DE35540122F1F7B38953F0BB0158319997338846 86C1A9019034D2CC113F81245F53B84EDD02B8ADB94638D40
Malicious:	**true**
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>401 Unauthorized</title>.</head><body>. Unauthorized . This server could not verify that you.are authorized to access the document.requested. Either you supplied the wrong.credentials (e.g., bad password), or your.browser doesn't understand how to supply.the credentials required. .</body></html>.

C:\Users\user\Desktop\rad75349.tmp.dll

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	316928
Entropy (8bit):	7.337848702590508
Encrypted:	false
SSDEEP:	6144:cwNQMQTlfdUPABVy559hhR3iP7TfPYbrF1EFVw0todxKROsCt:rNbadDBkZ6rPeEFizdxxsCt
MD5:	BFC060937DC90B273ECCB6825145F298
SHA1:	C156C00C7E918F0CB7363614FB1F177C90D8108A
SHA-256:	2F39C2879989DDD7F9ECF52B6232598E5595F8BF367846FF188C9DFBF1251253
SHA-512:	CC1FEE19314B0A0F9E292FA84F6E98F087033D77DB937848DDA1DA0C88F49997866CBA5465DF04BF929B810B42FDB81481341064C4565C9B6272FA7F3B473AC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L`.=...n...n...nCy.o...nCy.o...nCy.o...n.z.o(..n.z.o...n.z.o...nCy.o...n ...nq..n.z.o...n.z.o...n.zsn...n...n...n.z.o...nRich...n.....PE..d....6.d....." ...!.F.....0..... .....T...d...d....`..(. ...0..... .....8.....p...@.....`..`.....text....D.....F..... ..`.rdata.....`.....J.....@..@.data.....@....pdata.....0 .....@..@_RDATA..\....P.....@..@.rsrc...(....`.....@..@.reloc..... .....@..B..... .....

C:\Users\user\Documents\Outlook Files\Outlook Data File - NoEmail.pst	
Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	5139
Entropy (8bit):	1.8507519303077096
Encrypted:	false
SSDEEP:	24:Wc/c7JJJPfffffH/jCzDPLAh9ECN/+mMcoqqxGU5nuIIHq+NX9:YNfffffHOriv8xmIID9
MD5:	93EDBC6244E8383ED60A93DF93EA281C
SHA1:	0BB0BC49B90C8D15BDD689A740966BF9610A6F1F
SHA-256:	E32D3D4439E07830ADC99B5660C3195D6DE0CFDC10310711D137842D3B6EDA2D
SHA-512:	4DCDFD96F36EB44C639A82202E2BAD9D254EEBF943C3308078BCC7DFD05AAEC2522C28D26730C87E76849BAD2C98CD8E2BDC85B952682C22429D26904C5B0E9
Malicious:	false
Preview:	.....F.....".....\.....@.....f..... .....h.....\.....@. .....s...`.....$.....b.....f.....l..... .....y.....r.....`.....D...s...d.....p.....s...|.....s...|.....s...|.....s...|.....s...|.....s..... .....<.....<.....n...s...D.....@S.....s.....

C:\Windows\System32\BlUwZJEPejvMeG\xhwdmo.dll (copy)	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	316928
Entropy (8bit):	7.337848702590508
Encrypted:	false
SSDEEP:	6144:cwNQMQTlfdUPABVy559hhR3iP7TfPYbrF1EFVw0todxKROsCt:rNbadDBkZ6rPeEFizdxxsCt
MD5:	BFC060937DC90B273ECCB6825145F298
SHA1:	C156C00C7E918F0CB7363614FB1F177C90D8108A
SHA-256:	2F39C2879989DDD7F9ECF52B6232598E5595F8BF367846FF188C9DFBF1251253
SHA-512:	CC1FEE19314B0A0F9E292FA84F6E98F087033D77DB937848DDA1DA0C88F49997866CBA5465DF04BF929B810B42FDB81481341064C4565C9B6272FA7F3B473AC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L`.=...n...n...nCy.o...nCy.o...nCy.o...n.z.o(..n.z.o...n.z.o...nCy.o...n ...nq..n.z.o...n.z.o...n.zsn...n...n...n.z.o...nRich...n.....PE..d....6.d....." ...!.F.....0..... .....T...d...d....`..(. ...0..... .....8.....p...@.....`..`.....text....D.....F..... ..`.rdata.....`.....J.....@..@.data.....@....pdata.....0 .....@..@_RDATA..\....P.....@..@.rsrc...(...`.....@..@.reloc..... .....@..B.....

Static File Info

General

File type:	HTML document, ASCII text, with very long lines (792), with CRLF line terminators
Entropy (8bit):	5.21695797640856
TrID:	
File name:	click.wsf
File size:	55114
MD5:	016fa961b9af49d75b597c2f61ab344c
SHA1:	2fee0634cfa2988ee8f000724efc1c6c18beef23
SHA256:	8343af0017ad64499072d1485302948a7ad744a638bd2deab301ae108b6b18fd
SHA512:	4b58acb7111c383b0512352d86a3564d0a5167559d402d330ff7167a6e0ae2cf464096bba3a0936a566e3c2a9b0ffc4d448322c86658ed449e14fb46ad8fbdb8
SSDEEP:	768:w9Te2jdcdTeNtu1t/nl8BFWVyeaNhvsbsS:QTVdaeNtuXndH
TLSH:	313362F0AC025C0AE123D977B1BB561359C052FD42683B26FC6D507AE678E3096DD8EB
File Content Preview:	<job id="1cucuparu">..<script language="VBScript">..fastenedy = fastenedy + ("\ocw40599\ocw39558\ocw37476\ocw34353\ocw38517\ocw40599\ocw38170\ocw40252\ocw21167\ocw17003\ocw4511")..megamouthy = "megamouthy"..girlohy = girlohy + ("sycrwf\ocwfalsetreatedyext

File Icon

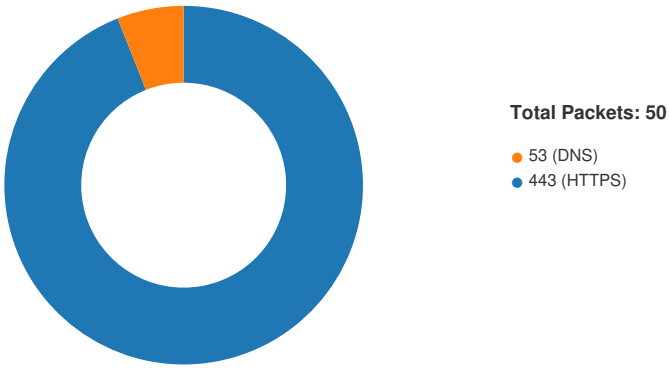
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3187.63.160.88 49735802404314 03/20/23-09:07:57.133517	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49735	80	192.168.2.3	187.63.160.88
192.168.2.3182.162.143.56497344432404312 03/20/23-09:07:41.132019	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49734	443	192.168.2.3	182.162.143.56
192.168.2.3104.168.155.143497388080240430 2 03/20/23-09:08:15.086032	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49738	8080	192.168.2.3	104.168.155.143
192.168.2.391.121.146.47 4973180802404344 03/20/23-09:07:19.650620	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49731	8080	192.168.2.3	91.121.146.47
192.168.2.3164.90.222.65 497374432404308 03/20/23-09:08:10.886539	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49737	443	192.168.2.3	164.90.222.65
192.168.2.3167.172.199.165497368080240431 0 03/20/23-09:08:05.635641	TCP	2404310	ET CNC Feodo Tracker Reported CnC Server TCP group 6	49736	8080	192.168.2.3	167.172.199.165
192.168.2.366.228.32.314 973370802404330 03/20/23-09:07:25.133944	TCP	2404330	ET CNC Feodo Tracker Reported CnC Server TCP group 16	49733	7080	192.168.2.3	66.228.32.31

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:06:37.277081966 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:37.277157068 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:37.277278900 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:37.281250954 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:37.281287909 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:37.856724977 CET	443	49727	203.26.41.131	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:06:37.856918097 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:37.862493992 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:37.862519979 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:37.862912893 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:37.902910948 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:38.086049080 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:38.086101055 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:38.453761101 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:38.453893900 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:38.454015970 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:38.454215050 CET	49727	443	192.168.2.3	203.26.41.131
Mar 20, 2023 09:06:38.454250097 CET	443	49727	203.26.41.131	192.168.2.3
Mar 20, 2023 09:06:38.756974936 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:38.757046938 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:38.757178068 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:38.758169889 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:38.758207083 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:38.898732901 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:38.898938894 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:38.901292086 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:38.901318073 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:38.901609898 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:38.902482033 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:38.902502060 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:39.005121946 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:39.005261898 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:39.005364895 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:39.007162094 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:39.007194042 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:39.007216930 CET	49728	443	192.168.2.3	31.31.196.172
Mar 20, 2023 09:06:39.007227898 CET	443	49728	31.31.196.172	192.168.2.3
Mar 20, 2023 09:06:39.700891018 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:39.700946093 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:39.701098919 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:39.711879969 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:39.711910009 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.441551924 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.441704988 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:40.444323063 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:40.444350958 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.444715023 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.445736885 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:40.445763111 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.871501923 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.871726036 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.871889114 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:40.871921062 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:40.921637058 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.103441954 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.103568077 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.103580952 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.103604078 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.103643894 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.103651047 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.103668928 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.103671074 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.103719950 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.103815079 CET	443	49729	186.202.153.5	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:06:41.103898048 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.335499048 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.335558891 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.335699081 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.335710049 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.335740089 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.335784912 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.335819006 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.335894108 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.336009026 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.336385965 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.336483002 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.336533070 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.336610079 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.336978912 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.337086916 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.567697048 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.567724943 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.567856073 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.567913055 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.567944050 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.568010092 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.568078041 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.568078995 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.568108082 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.568233967 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.568310022 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.568434954 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.568497896 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.568624020 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.568809986 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.568912029 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.569062948 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.569207907 CET	49729	443	192.168.2.3	186.202.153.5
Mar 20, 2023 09:06:41.569339991 CET	443	49729	186.202.153.5	192.168.2.3
Mar 20, 2023 09:06:41.569442987 CET	49729	443	192.168.2.3	186.202.153.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:06:36.428728104 CET	60008	53	192.168.2.3	1.1.1.1
Mar 20, 2023 09:06:37.266818047 CET	53	60008	1.1.1.1	192.168.2.3
Mar 20, 2023 09:06:38.496239901 CET	53710	53	192.168.2.3	1.1.1.1
Mar 20, 2023 09:06:38.754851103 CET	53	53710	1.1.1.1	192.168.2.3
Mar 20, 2023 09:06:39.017168045 CET	55103	53	192.168.2.3	1.1.1.1
Mar 20, 2023 09:06:39.699096918 CET	53	55103	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 09:06:36.428728104 CET	192.168.2.3	1.1.1.1	0x4e7e	Standard query (0)	penshorn.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:06:38.496239901 CET	192.168.2.3	1.1.1.1	0x4d17	Standard query (0)	bbvoyage.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:06:39.017168045 CET	192.168.2.3	1.1.1.1	0x8dc3	Standard query (0)	www.gomespontes.com.br	A (IP address)	IN (0x0001)	false

DNS Answers

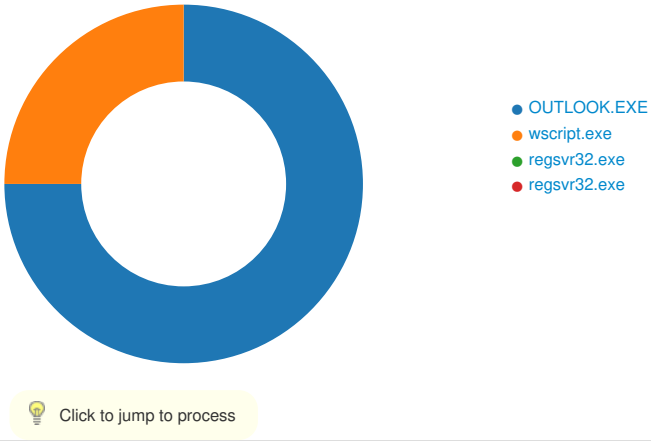
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 09:06:37.266818047 CET	1.1.1.1	192.168.2.3	0x4e7e	No error (0)	penshorn.org		203.26.41.131	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:06:38.754851103 CET	1.1.1.1	192.168.2.3	0x4d17	No error (0)	bbvoyage.com		31.31.196.172	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:06:39.699096918 CET	1.1.1.1	192.168.2.3	0x8dc3	No error (0)	www.gomespontes.com.br	gomespontes.com.br		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:06:39.699096918 CET	1.1.1.1	192.168.2.3	0x8dc3	No error (0)	gomespontes.com.br		186.202.153.5	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- penshorn.org
- bbvoyage.com
- www.gomespontes.com.br
- 164.90.222.65

Statistics

Behavior



System Behavior

Analysis Process: OUTLOOK.EXE PID: **804**, Parent PID: **-1**

General	
Target ID:	0
Start time:	09:06:33
Start date:	20/03/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail

Imagebase:	0x7ff64d520000
File size:	41778000 bytes
MD5 hash:	CA3FDE8329DE07C95897DB0D828545CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_Accessibility_ReminderType	unicode	{"name":"Accessibility_ReminderType","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF64D7CBB70	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings	Accounts	unicode	[]	[{"scope":"","userUpn":"","accountAge":0,"timestamp":0,"anchorMailbox":"","roamingStatus":"LOCAL"}]	success or wait	1	7FF64D7CBE60	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_AccountsNeedResyncing	unicode	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"false","isFirstSync":"false","source":""}	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF64D7CBB70	RegSetValueExW

Analysis Process: wscript.exe PID: **6404**, Parent PID: **3840**

General

Target ID:	1
Start time:	09:06:34
Start date:	20/03/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\click.wsf"
Imagebase:	0x7ff7e91a0000
File size:	165888 bytes
MD5 hash:	563EDAE37876138FDFF47F3E7A9A78FD

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1414548751.000002D845C7D000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: WEBSHELL_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000001.00000002.1552503322.000002D84653C000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1530447488.000002D846461000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: WEBSHELL_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000001.00000003.1530447488.000002D846461000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1411114207.000002D845CCE000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1413926742.000002D845C7D000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1410988197.000002D845C7D000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1411114207.000002D845C7D000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1533460578.000002D84653C000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: WEBSHELL_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000001.00000003.1533460578.000002D84653C000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1412954439.000002D845C7D000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: WEBSHELL_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000001.00000003.1542433572.000002D84653C000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 00000001.00000003.1414114730.000002D845C7D000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\click.wsf	0	9	62 61 64 75 6d 20 74 73 73	badum tss	success or wait	1	7FFFC4E442B8	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6508**, Parent PID: **6404**

General

Target ID:	3
Start time:	09:06:41
Start date:	20/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe" "C:\Users\user\Desktop\rad75349.tmp.dll
Imagebase:	0x7ff6d5170000
File size:	24064 bytes
MD5 hash:	578BAB56836A3FE455FFC7883041825B
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: 00000003.00000002.1502600709.0000000000731000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.1501910088.0000000000460000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

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: **6544**, Parent PID: **6508**

General

Target ID:	4
Start time:	09:06:44
Start date:	20/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\BlUwZJEPejvMeG\xhwdmo.dll"
Imagebase:	0x7ff6d5170000
File size:	24064 bytes
MD5 hash:	578BAB56836A3FE455FFC7883041825B
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: 00000004.00000002.2660986060.0000000000C99000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly