ID: 356494
Sample Name: PO_210223.exe
Cookbook: default.jbs
Time: 08:57:40
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

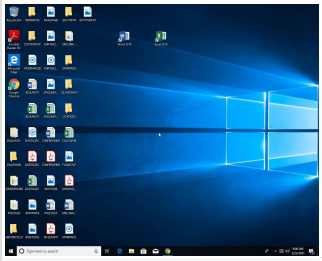
Analysis Report PO_210223.exe

Overview

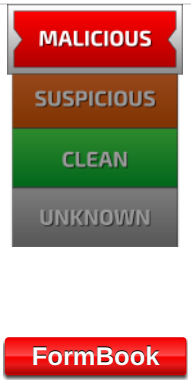
General Information

Sample Name:	PO_210223.exe
Analysis ID:	356494
MD5:	e40af9745e938b7.
SHA1:	d9e750061417b0..
SHA256:	38acc90cd6d33b...
Tags:	exe Formbook geo KOR

Most interesting Screenshot:



Detection



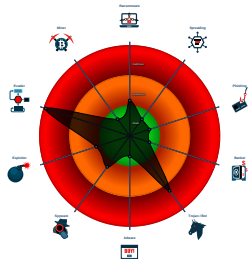
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- PO_210223.exe (PID: 6976 cmdline: 'C:\Users\user\Desktop\PO_210223.exe' MD5: E40AF9745E938B72D5D860BBC679AEBF)
  - schtasks.exe (PID: 1556 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kwqifureL' /XML 'C:\Users\user\AppData\Local\Temp\tmp33D2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PO_210223.exe (PID: 1868 cmdline: C:\Users\user\Desktop\PO_210223.exe MD5: E40AF9745E938B72D5D860BBC679AEBF)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 6744 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 7112 cmdline: /c del 'C:\Users\user\Desktop\PO_210223.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.000666dy.com/ntg/"
  ],
  "decoy": [
    "successwithyolandafgreen.com",
    "theordinaryph.com",
    "atamyo-therapeutics.com",
    "pophazard.com",
    "anthonyfultz.com",
    "pasanglham.com",
    "kanekhushi.com",
    "littlefishyswim.com",
    "kaieteurny.com",
    "fanavartima.com",
    "digexpo.com",
    "se-rto.com",
    "chaos.finance",
    "bakldx.com",
    "after-school.pro",
    "faithfromphilly.com",
    "estudiomuradian.com",
    "albertocerasini.com",
    "andronna.com",
    "wingspotusa.com",
    "lucky-lucky.online",
    "ga-don.com",
    "shawnbly.com",
    "shoptalullah.com",
    "needfulvegan.com",
    "ampersandaconsulting.com",
    "hoyhelp.com",
    "wickfordinternists.com",
    "kindlovingmindfulyoga.com",
    "hhkgjt.net",
    "eventpubgpharaoh.com",
    "blameitonpizza.com",
    "editshirt.com",
    "utulocal194.com",
    "meralpro.com",
    "rochesterhindus.com",
    "wadihassafi.com",
    "visitouroffice.com",
    "duncantraining.com",
    "ggrealestategroup.com",
    "xrf-tech.com",
    "pro-tizer.com",
    "usesoft.icu",
    "caralsalem.com",
    "inudaipur.com",
    "fluid-branding.com",
    "titizadiyamancigkofte.com",
    "es-tucasa.com",
    "103manningave.com",
    "eclat-beauty.info",
    "ahameeting2021.com",
    "gsyxh.com",
    "246835.com",
    "onwardfpv.com",
    "estasinvitado.net",
    "kinderkakery.com",
    "bala5.com",
    "gehqaralouine.com",
    "editorialesrd.com",
    "thebarconcepts.com",
    "aleitzeventdecor.com",
    "moderaty.com",
    "geraloqaresuine.com",
    "kyotodreaming.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.715452206.0000000001180000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.715452206.0000000001180000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.715452206.0000000001180000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
0000000D.00000002.907288680.000000000009B0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000002.907288680.000000000009B0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO_210223.exe.2cb671c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.PO_210223.exe.45c8e00.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.PO_210223.exe.45c8e00.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xe6998:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xe6c02:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x112fb8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x113222:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xf2725:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x11ed45:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xf2211:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x11e831:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xf2827:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x11ee47:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xf299f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x11efbf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xe761a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x113c3a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xf148c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x11daac:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xe8313:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x114933:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xf83c7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1249e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xf93ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.PO_210223.exe.45c8e00.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xf54a9:$sqlite3step: 68 34 1C 7B E1 • 0xf55bc:$sqlite3step: 68 34 1C 7B E1 • 0x121ac9:$sqlite3step: 68 34 1C 7B E1 • 0x121bdc:$sqlite3step: 68 34 1C 7B E1 • 0xf54d8:$sqlite3text: 68 38 2A 90 C5 • 0xf55fd:$sqlite3text: 68 38 2A 90 C5 • 0x121af8:$sqlite3text: 68 38 2A 90 C5 • 0x121c1d:$sqlite3text: 68 38 2A 90 C5 • 0xf54eb:$sqlite3blob: 68 53 D8 7F 8C • 0xf5613:$sqlite3blob: 68 53 D8 7F 8C • 0x121b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x121c33:$sqlite3blob: 68 53 D8 7F 8C

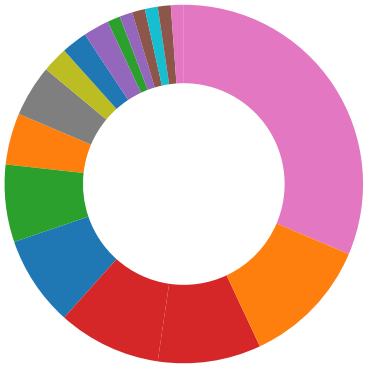
Source	Rule	Description	Author	Strings
9.2.PO_210223.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 8 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

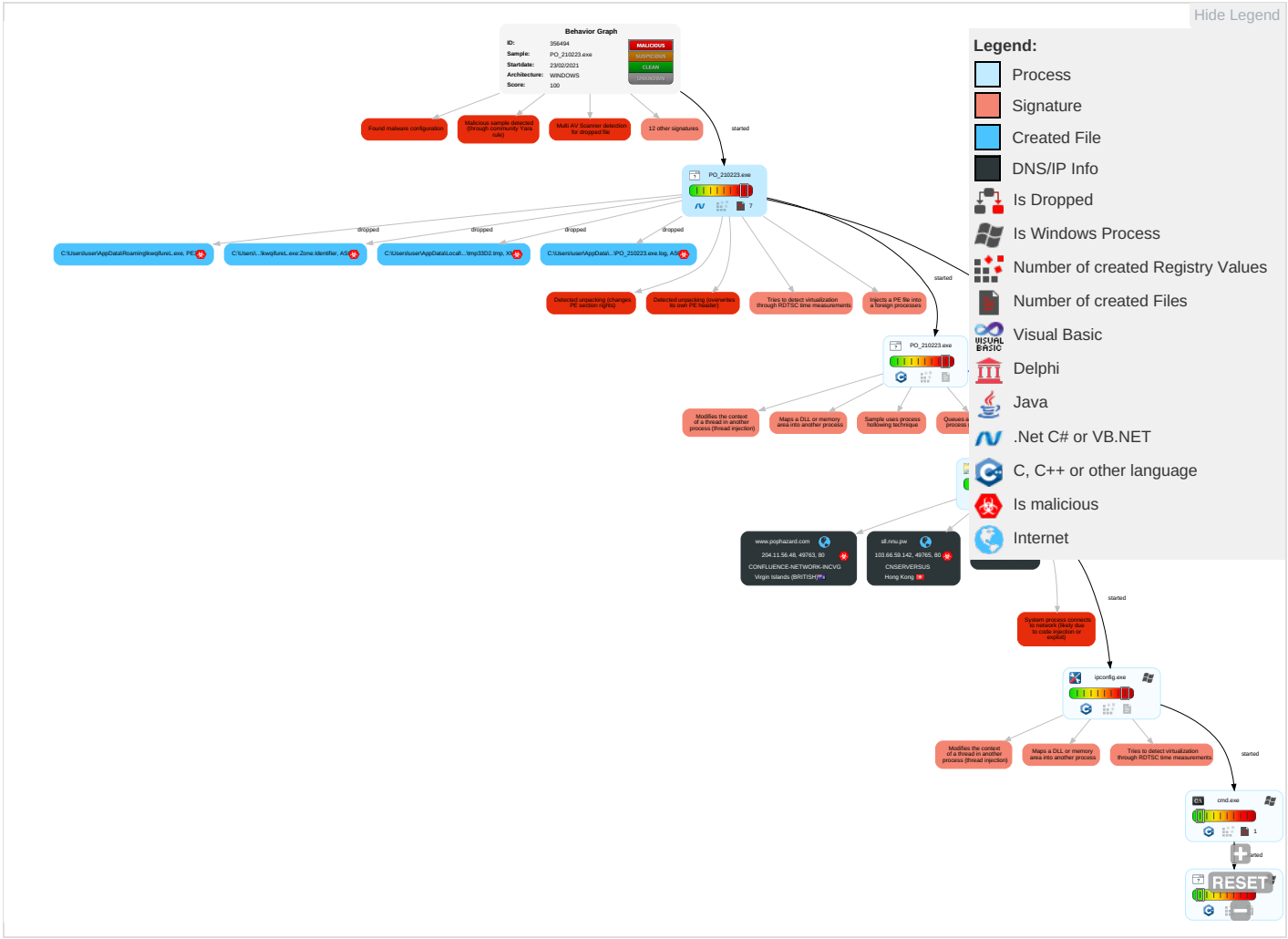
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	Input Capture 1	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

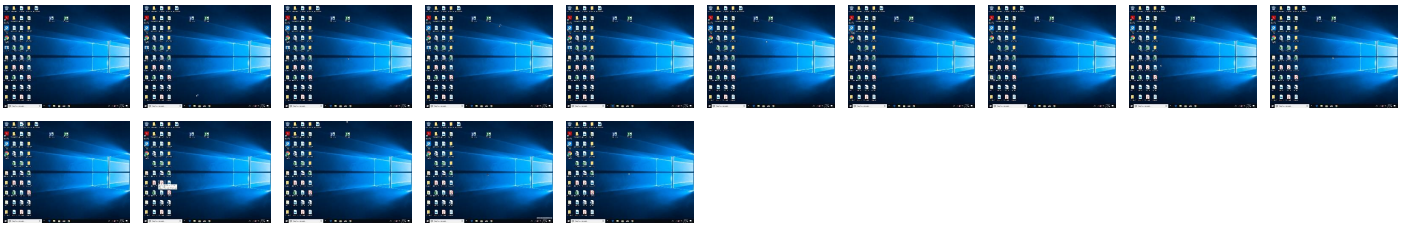
Behavior Graph



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
PO_210223.exe	31%	Virustotal		Browse
PO_210223.exe	43%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
PO_210223.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kwqifureL.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kwqifureL.exe	43%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.PO_210223.exe.890000.0.unpack	100%	Avira	HEUR/AGEN.1134873		Download File
9.2.PO_210223.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
kaieteurny.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnal	0%	Avira URL Cloud	safe	
http://www.pophazard.com/ntg/?ojoHzZ=ezEzfTUVqdhTeHhhSUO1nROjhCSdyq2ILgetv621tco9QxJ0Ek6h+l0QSU1+LT7ErdbR&1bm=GPD0lNKPfFHTAb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.otf	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/pics/12471/kwbg.jpg)	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.ttf	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/pics/12471/arrow.png)	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/pics/12471/libgh.png)	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/logo.png)	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comig	0%	Avira URL Cloud	safe	
http://www.246835.com/ntg/?ojoHzZ=w4X+hAUHJfroJmp94c1onPOAPenZZpTxtRzXhSWsn9e2URXOAMjiMifVYC4X6954J+Dz&1bm=GPD0lNKPfFHTAb	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva9y	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcy	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/bodybg.png)	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot	0%	Avira URL Cloud	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/pics/12471/search-icon.png)	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.ttf	0%	Avira URL Cloud	safe	
http://www.kaieteurny.com/ntg/?ojoHzZ=bxqEOtZwpu8QOdqfa5M05y7zdw+lGZ3K+8kzjODwarG6Nc6O9nhCMo5PAGRXJYSnY3HU&1bm=GPD0lNKPfFHTAb	0%	Avira URL Cloud	safe	
www.000666dy.com/ntg/	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.otf	0%	Avira URL Cloud	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cniy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comint	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/pics/12471/libg.png)	0%	Avira URL Cloud	safe	
http://www.tiro.comal	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.pophazard.com/sk-logabpstatus.php?a=aG42QXdLZEpxVDR5Y2RqNUtBbnIvaUNNaWJVdEVQVjlJMUxVR2dwW	0%	Avira URL Cloud	safe	
http://www.tiro.com8i	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kaieteurny.com	23.229.197.103	true	true	• 0%, Virustotal, Browse	unknown
sll.nnu.pw	103.66.59.142	true	true		unknown
www.pophazard.com	204.11.56.48	true	true		unknown
www.246835.com	unknown	unknown	true		unknown
www.kaieteurny.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.pophazard.com/ntg/?ojoHzZ=ezEzfTUVqdhTeHhhSUO1nROjhCSdyq2ILgetv621tco9QxJ0Ek6h+l0QSU1+LT7ErdbR&1bm=GPD0lNKPfFHTAb	true	• Avira URL Cloud: safe	unknown
http://www.246835.com/ntg/?ojoHzZ=w4X+hAUHJfroJmp94c1onPOAPenZZpTxtRzXhSWsn9e2URXOAMjiMifVYC4X6954J+Dz&1bm=GPD0lNKPfFHTAb	true	• Avira URL Cloud: safe	unknown
http://www.kaieteurny.com/ntg/?ojoHzZ=bxqEOtZwpu8QOdqfa5M05y7zdw+lGZ3K+8kzjODwarG6Nc6O9nhCMo5PAGRXJYSnY3HU&1bm=GPD0lNKPfFHTAb	true	• Avira URL Cloud: safe	unknown
www.000666dy.com/ntg/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnal	PO_210223.exe, 00000000.00000003.647755183.0000000008255000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	PO_210223.exe, 00000000.00000003.658952636.0000000008285000.00000004.00000001.sdmp, PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.otf	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i3.cdn-image.com/__media__/pics/12471/kwbg.jpg)	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

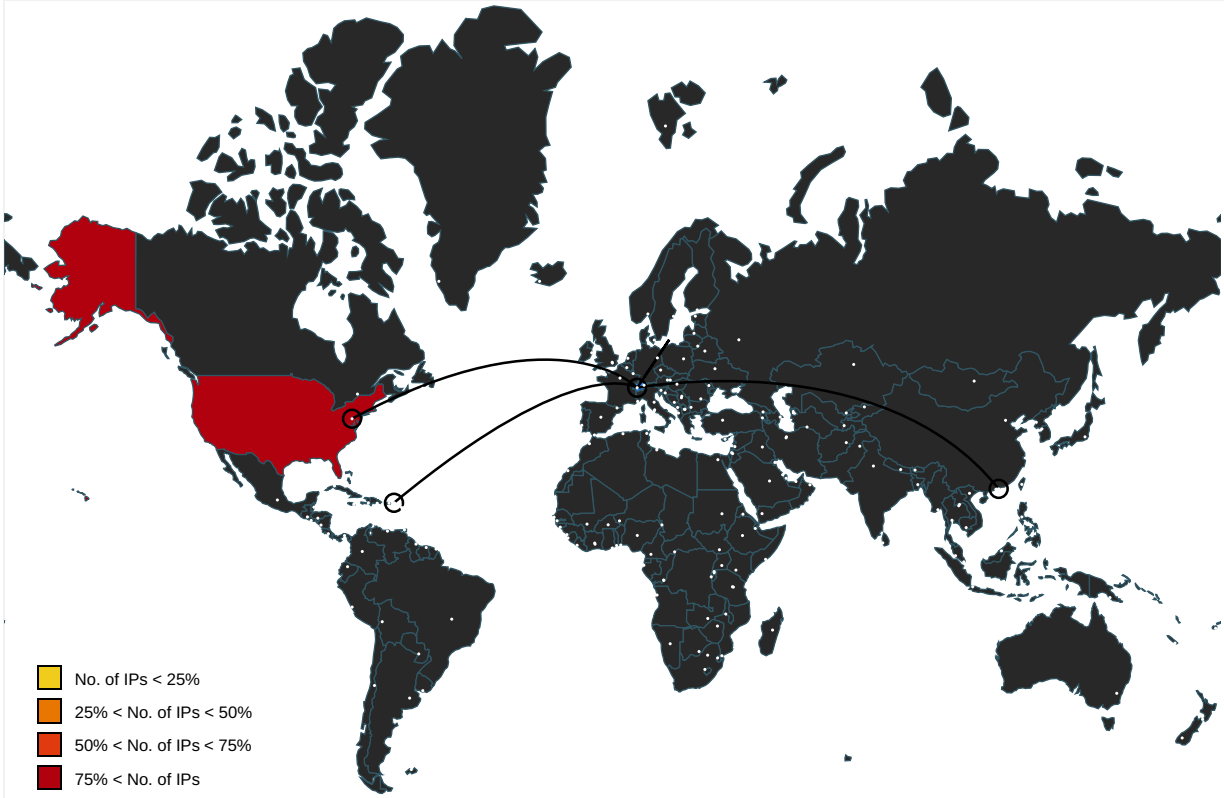
Name	Source	Malicious	Antivirus Detection	Reputation
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.ttf	ipconfig.exe, 0000000D.0000000 2.911031033.0000000003E4F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com	PO_210223.exe, 00000000.000000 03.648938805.0000000008252000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersQ	PO_210223.exe, 00000000.000000 03.654377069.0000000008285000. 00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersiva	PO_210223.exe, 00000000.000000 03.658952636.0000000008285000. 00000004.00000001.sdmp	false		high
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	PO_210223.exe, 00000000.000000 02.680445109.0000000002C2D000. 00000004.00000001.sdmp	false		high
http://i3.cdn-image.com/__media__/pics/12471/arrow.png)	ipconfig.exe, 0000000D.0000000 2.911031033.0000000003E4F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	PO_210223.exe, 00000000.000000 02.686743124.0000000009462000. 00000004.00000001.sdmp, explor er.exe, 0000000A.00000000.6969 26398.000000000B970000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PO_210223.exe, 00000000.000000 02.686743124.0000000009462000. 00000004.00000001.sdmp, explor er.exe, 0000000A.00000000.6969 26398.000000000B970000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PO_210223.exe, 00000000.000000 02.686743124.0000000009462000. 00000004.00000001.sdmp, explor er.exe, 0000000A.00000000.6969 26398.000000000B970000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO_210223.exe, 00000000.000000 03.655856986.0000000008285000. 00000004.00000001.sdmp, PO_210 223.exe, 00000000.00000002.686 743124.0000000009462000.000000 04.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398. 000000000B970000.00000002.0000 0001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PO_210223.exe, 00000000.000000 02.686743124.0000000009462000. 00000004.00000001.sdmp, PO_210 223.exe, 00000000.00000003.646 155016.000000000826B000.000000 04.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398. 000000000B970000.00000002.0000 0001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	PO_210223.exe, 00000000.000000 03.645842271.000000000826B000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i3.cdn-image.com/__media__/pics/12471/libgh.png)	ipconfig.exe, 0000000D.0000000 2.911031033.0000000003E4F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i3.cdn-image.com/__media__/pics/12471/logo.png)	ipconfig.exe, 0000000D.0000000 2.911031033.0000000003E4F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerse	PO_210223.exe, 00000000.000000 03.658906996.0000000008285000. 00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	PO_210223.exe, 00000000.000000 02.686743124.0000000009462000. 00000004.00000001.sdmp, explor er.exe, 0000000A.00000000.6969 26398.000000000B970000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 0000000A.0000000 2.910436982.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	PO_210223.exe, 00000000.000000 02.686743124.0000000009462000. 00000004.00000001.sdmp, explor er.exe, 0000000A.00000000.6969 26398.000000000B970000.0000000 2.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot?#iefix	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO_210223.exe, 00000000.00000003.648938805.0000000008252000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO_210223.exe, 00000000.00000002.680445109.0000000002C2D000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comig	PO_210223.exe, 00000000.00000003.648155639.000000000828D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comva9y	PO_210223.exe, 00000000.00000003.648938805.0000000008252000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comcy	PO_210223.exe, 00000000.00000003.648075554.000000000828D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://i3.cdn-image.com/__media__/pics/12471/bodybg.png)	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comc	PO_210223.exe, 00000000.00000003.645891455.000000000826B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i3.cdn-image.com/__media__/pics/12471/search-icon.png)	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comlic	PO_210223.exe, 00000000.00000003.649005992.0000000008252000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.ttf	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot?#iefix	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.otf	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comk	PO_210223.exe, 00000000.00000003.648938805.0000000008252000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	PO_210223.exe, 00000000.00000003.647493837.0000000008252000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cniy	PO_210223.exe, 00000000.00000003.648938805.0000000008252000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comint	PO_210223.exe, 00000000.00000003.648075554.000000000828D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	PO_210223.exe, 00000000.00000003.648938805.0000000008252000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://i3.cdn-image.com/__media__/pics/12471/libg.png)	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comal	PO_210223.exe, 00000000.00000003.646155016.000000000826B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	PO_210223.exe, 00000000.00000003.658733903.0000000008285000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pophazard.com/sk-logabpstatus.php?a=aG42QXdLZEpxVDR5Y2RqNUtBbnIvaUNNaWJVdEVQVjlJMUxVR2dwW	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com8i	PO_210223.exe, 00000000.00000003.649005992.0000000008252000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	PO_210223.exe, 00000000.00000002.686743124.0000000009462000.00000004.00000001.sdmp, explorer.exe, 0000000A.00000000.696926398.000000000B970000.00000002.00000001.sdmp	false		high
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.svg#ubuntu-b	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.svg#ubuntu-r	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comh	PO_210223.exe, 00000000.00000003.646155016.000000000826B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff2	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnal9y	PO_210223.exe, 00000000.00000003.647493837.0000000008252000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	PO_210223.exe, 00000000.00000003.652634958.0000000008285000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff2	ipconfig.exe, 0000000D.00000002.911031033.0000000003E4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnt7o	PO_210223.exe, 00000000.00000003.647129278.0000000008256000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.11.56.48	unknown	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
103.66.59.142	unknown	Hong Kong		40065	CNSERVERSUS	true
23.229.197.103	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356494
Start date:	23.02.2021
Start time:	08:57:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO_210223.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	23
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.evad.winEXE@10/4@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.7% (good quality ratio 12.2%) • Quality average: 64.6% • Quality standard deviation: 36.1%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 51.104.139.180, 52.113.196.254, 104.43.139.144, 92.122.145.220, 168.61.161.212, 205.185.216.10, 205.185.216.42, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.144.132 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:58:35	API Interceptor	1x Sleep call for process: PO_210223.exe modified

Time	Type	Description

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
204.11.56.48	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• www.bigias.com/dgn/?Yzrp=LfNQbftNF2CZK3Pdbvfs/GUpg4UhIVB9HREii+G/2FPSQnC/ZhagFrpEcGqY3PnsjIPUew==&Lzrl=k6fTBXMx9H
	8nxKYwJna8.exe	Get hash	malicious	Browse	• www.wood-decor24.com/csv8/?UT=EhUhb4&OjKL3=3r5dRtIFgT1VahUseje8ue8NA/87jk0khJCRLUJpCdq1RUr7MGeMpqJjvp2wRjK1uE1w
	win32.exe	Get hash	malicious	Browse	• www.buythinsecret.com/incn/?8pBP5p=TJfvpzXJMrBT1in/CsTGivtbaFX6GTyf1u5RDlluSiJ51lGqZDPSCkL06IZ75j/ocR9F&L6Ah=2dSLFXghYtFd0
	mitbjisfe.js	Get hash	malicious	Browse	• urchintelemetry.com/
	Details...exe	Get hash	malicious	Browse	• www.coolgadgetsdominate.com/t052/?pPX=6CpI00+2HCKGB1JbH22k369411uOsTuNarkGYMnsdTbHzEXKI/PSljtTQWzMzlp4SIHA&1b=jnKtRfexr
	Fdj5vhj87S.exe	Get hash	malicious	Browse	• www.buythinsecret.com/incn/?2de=TJfvpzXJMrBT1in/CsTGivtbaFX6GTyf1u5RDlluSiJ51lGqZDPSCkL06L5BpyfQG2cC&2dpxxT=i6MpbxRhTzX8wRbP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Statement Of Account.exe	Get hash	malicious	Browse	• www.perphaseelectronics.com/sz0m/?Kh=HN60TPe8&GvIHh=TGzqOvQKUvlZAzOTrBjC19//UpjckKets6PHJd4ZAWTshAj7ZEPkQjl0VseEDOP7xUYnlWwQiw==
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• www.wood-decor24.com/csv8/?Aro=3r5dRtIFgT1VahUsje8ue8NA/87jk0khJCRLUJpCdq1RUr7MGeMpqJjvqaKSimOtzUhnn+APQ==&EHU40X=gbWtoXjpHB
	spptqzbEyNlEJvj.exe	Get hash	malicious	Browse	• www.become-flightattendant.com/umSa/?Bn=d8+Yc1Kqdgg0yWZra+sA0ykjlSaGatnyagLIGXz6lWosdhkxYMJxV2/awb2OazI1/ohH&Rv=Y2JToVAX_DCpOHB
	pHUWiFd56t.exe	Get hash	malicious	Browse	• www.wood-decor24.com/csv8/?Rxl=3r5dRtIFgT1VahUsje8ue8NA/87jk0khJCRLUJpCdq1RUr7MGeMpqJjvqWKByqN0jU3&LJB=GbtlyLR0j
	Q38V8rfl5H.js	Get hash	malicious	Browse	• legitville.com/0.html
	Q38V8rfl5H.js	Get hash	malicious	Browse	• legitville.com/0.html
	Z4VzMe8lqZ.js	Get hash	malicious	Browse	• urchintelemetry.com/
	Z4VzMe8lqZ.js	Get hash	malicious	Browse	• urchintelemetry.com/
	test.bat	Get hash	malicious	Browse	• local-update.com/banana.png
	SecuriteInfo.com.Heur.16160.xls	Get hash	malicious	Browse	• www.heretangier.com/p2he/?cF=CXY0HpOvAiNao/7hyD46ZbvJkOBYOaiMbMD/1gQDGANTp/VCja9vaOiD7B1AqPi5K6pAxQ==&SBZ=epg8b
	YT0nfh456s.exe	Get hash	malicious	Browse	• www.wood-decor24.com/csv8/?jFNHHj=3r5dRtIFgT1VahUseje8ue8NA/87jk0khJCRLUJpCdq1RUr7MGeMpqJjvqWKByqN0jU3&Ppd=_6g8yvxH-6HLN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	payment advise.exe	Get hash	malicious	Browse	• www.couponquote.com/rbe/?8pV=_TJP3HkXZXxT3Te&lJBxWNm=NmtmFq3bM1GRjzQAFWXZGZs3nJJTmL04NhsM+Fht47V2qooXGZt1Rr5A9fSZbB9GvZz2
	NEW URGENT ORDER FROM PUK ITALIA GROUP SRL.EXE	Get hash	malicious	Browse	• www.starstylishinstitute.com/k47/?r6=GbwDj4ypT&-ZU=33t3A7xB80u5YuyQF102BXSRJYIHEjWKu55cOthnVryNN9gNL+MJJIyFRKYoAf86uF3O
	Spisemuligheds4.exe	Get hash	malicious	Browse	• www.momentsbyjordan.com/gpb6/?SBtxlt=lxlHQfw0FrIH&2d=gqgpWAjeEz0jXgJI2O1sVbKbB5UJYpIgFLCmC8Bdjh8wHvxJiiG9zRydokK2P49lkh4X

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CONFLUENCE-NETWORK-INCVG	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 208.91.197.91
	X1(1).xlsm	Get hash	malicious	Browse	• 66.81.204.228
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 204.11.56.48
	X1(1).xlsm	Get hash	malicious	Browse	• 66.81.204.228
	DHL Document. PDF.exe	Get hash	malicious	Browse	• 208.91.197.91
	X1(1).xlsm	Get hash	malicious	Browse	• 66.81.204.228
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 208.91.197.27
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 66.81.204.228
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 66.81.204.228
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 66.81.204.228
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 66.81.204.228
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 66.81.204.228
	HEC Batangas Integrated LNG and Power Project DocumentationsType a message.exe.exe	Get hash	malicious	Browse	• 208.91.197.39
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 208.91.197.91
	0C18PUs3bt.exe	Get hash	malicious	Browse	• 208.91.197.27
	Quotation.exe	Get hash	malicious	Browse	• 209.99.64.55
	Credit Card & Booking details.exe	Get hash	malicious	Browse	• 208.91.197.27
	DnHel10lQ6.exe	Get hash	malicious	Browse	• 209.99.40.222
	Quotation.exe	Get hash	malicious	Browse	• 209.99.64.55
	Payment advice.xls	Get hash	malicious	Browse	• 209.99.40.222
CNSERVERSUS	DHL Document. PDF.exe	Get hash	malicious	Browse	• 154.86.13.178
	SHED.EXE	Get hash	malicious	Browse	• 172.247.179.59
	#U6211#U662f#U56fe#U7247.exe	Get hash	malicious	Browse	• 23.224.244.116
	Parcel _009887 .exe	Get hash	malicious	Browse	• 45.205.32.159
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 154.91.163.79
	RFQ 2027376.xlsx	Get hash	malicious	Browse	• 23.224.206.44
	dll.dll	Get hash	malicious	Browse	• 154.222.24.167
	im.exe	Get hash	malicious	Browse	• 103.66.58.214

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8nxKYwJna8.exe	Get hash	malicious	Browse	• 156.251.194.127
	d6DdOfC2CX.exe	Get hash	malicious	Browse	• 154.202.47.2
	IRS_Microsoft_Excel_Document_xls.jar	Get hash	malicious	Browse	• 45.142.156.44
	WlBvCPCRcs.exe	Get hash	malicious	Browse	• 23.225.97.176
	8foMX5QfDT.exe	Get hash	malicious	Browse	• 104.255.229.20
	8GgbjB3BpU.exe	Get hash	malicious	Browse	• 172.83.155.157
	CMA CGM Shipping Documents COAU7014424560.xlsx	Get hash	malicious	Browse	• 23.225.97.176
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 154.91.154.163
	Report-preview01.20.exe	Get hash	malicious	Browse	• 172.83.155.149
	KtJsMM8kdE.exe	Get hash	malicious	Browse	• 156.251.194.127
	Fdj5vhj87S.exe	Get hash	malicious	Browse	• 154.91.154.163
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 104.255.229.21

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_210223.exe.log	
Process:	C:\Users\user\Desktop\PO_210223.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp33D2.tmp	
Process:	C:\Users\user\Desktop\PO_210223.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.176262409235197
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGGtn:cbhK79lNQR/rydbz9l3YODOLNdq3F
MD5:	14CFB330CC1F251E200D3DF339B27897
SHA1:	D203DB04E55F6224C704FBF3BF5A1654A22D4C24
SHA-256:	84CDADDE88E64BDF5193CBD7CA5FDAFF6C835E095EEE55053553413F7F3A588F
SHA-512:	EB556DCF6EAC7196F52C607803DFBE4DEF8B9346F5AA25FFE1B2BB850088E54524E6596F67B591BC0C2143B275C55001201B065E32CC752B197A30780B3BC2D
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp33D2.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\kwqifureL.exe	
Process:	C:\Users\user\Desktop\PO_210223.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.2424881132869325
Encrypted:	false
SSDEEP:	12288:9ORam/OrNbZTlgJqfsRVeh58JtAZUdt4odT9YdxOI/aFOAhIE+TtORqH4O4H1rVR:QFiJNlFfdkP4odidxTCEd2
MD5:	E40AF9745E938B72D5D860BBC679AEBF
SHA1:	D9E750061417B0CA9F933DB79C99C12934ABBE84
SHA-256:	38ACC90CD6D33B61B99CCA8CF06781E1BD2AB8FFEBC3A33E036ECA36037D413B
SHA-512:	2124A0CB2135BFC5731554AAA534E6BA9063137450E5DF18A56C8DD661D8D926278C1D658F1AEF44D3522598E047F4735CA5A06CEF41BE3593101A089F3494BA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Q4`.....P..*.....I... ...`....@.. ....@.....XI..S....`..... ..... ..H.....text....)... ...*..... ..`.rsrc.....`.....,.....@..@.reloc..... .....<.....@..B.....I.....H.....HY.....B....O..X.....kh.6.v.h.j...@..'.h.BD..c."~-...^.....r.S...R....!.Z...#i.....8..4.2,..5.aw!D...0.Z%....Z.w(....a ...y..u...?.[...j....a0.`2.\.....d..w..G..}.D....<..`.C.....A....5....s.A....U..Pff..DF.... N.g..e.(.....3.).<..;6.F.x%...q.f.=+.Q...../A1CHt....2....G?.+..m...3.G.B...*...i.A..C.....R. ..BE....R..b..1t....Z....z`..P.. ...~XS!R.(.....T.o....D...b..lM.<+0..p..$.fd.....H..j

C:\Users\user\AppData\Roaming\kwqifureL.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO_210223.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.2424881132869325
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO_210223.exe
File size:	802304
MD5:	e40af9745e938b72d5d860bbc679aebf
SHA1:	d9e750061417b0ca9f933db79c99c12934abbe84

General

SHA256:	38acc90cd6d33b61b99cca8cf06781e1bd2ab8ffebc3a33 e036eca36037d413b
SHA512:	2124a0cb2135bfc5731554aaa534e6ba9063137450e5df1 8a56c8dd661d8d926278c1d658f1aef44d3522598e047f4 735ca5a06cef41be3593101a089f3494ba
SSDEEP:	12288:9ORam/OrNbZTlgJqfsRVeh58JtAZUdt4odT9Ydx OI/aFOAhIE+TtORqH4O4H1rVR:QFiJNlFfdkP4odidxTC Ed2
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L.... Q4`..............P..*...........I... ...`....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c49ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60345188 [Tue Feb 23 00:51:20 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc4958	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0xfe8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc29b4	0xc2a00	False	0.699083273121	data	7.247286296	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0xfe8	0x1000	False	0.399658203125	data	5.00156812291	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc60a0	0x334	data		
RT_MANIFEST	0xc63d4	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

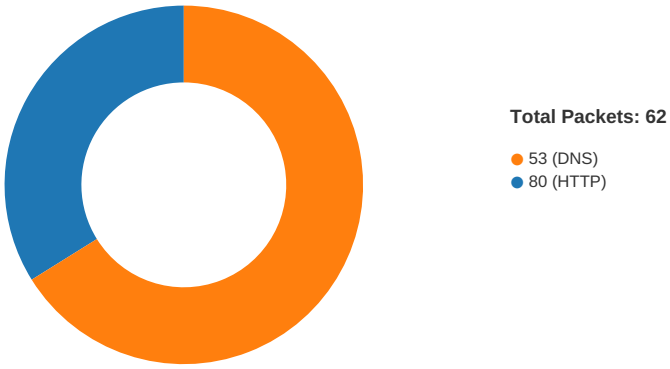
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	UCOMITypeComp.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB

Description	Data
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	UCOMITypeComp.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:59:45.696063042 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:45.858366966 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:45.858566999 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:45.858961105 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.021274090 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.287998915 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288073063 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288115978 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288146973 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288218975 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288261890 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288300037 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288306952 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.288347960 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.288388968 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.288444042 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.346735954 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.369762897 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.370002985 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.450568914 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.450594902 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.450609922 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.450627089 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.450850010 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.509321928 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.509608984 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 08:59:46.532135963 CET	80	49763	204.11.56.48	192.168.2.4
Feb 23, 2021 08:59:46.532339096 CET	49763	80	192.168.2.4	204.11.56.48
Feb 23, 2021 09:00:04.907589912 CET	49765	80	192.168.2.4	103.66.59.142
Feb 23, 2021 09:00:05.238830090 CET	80	49765	103.66.59.142	192.168.2.4
Feb 23, 2021 09:00:05.239036083 CET	49765	80	192.168.2.4	103.66.59.142
Feb 23, 2021 09:00:05.239259958 CET	49765	80	192.168.2.4	103.66.59.142
Feb 23, 2021 09:00:05.567799091 CET	80	49765	103.66.59.142	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:00:05.594891071 CET	80	49765	103.66.59.142	192.168.2.4
Feb 23, 2021 09:00:05.594916105 CET	80	49765	103.66.59.142	192.168.2.4
Feb 23, 2021 09:00:05.595118046 CET	49765	80	192.168.2.4	103.66.59.142
Feb 23, 2021 09:00:05.595191956 CET	49765	80	192.168.2.4	103.66.59.142
Feb 23, 2021 09:00:05.925678968 CET	80	49765	103.66.59.142	192.168.2.4
Feb 23, 2021 09:00:25.861310005 CET	49767	80	192.168.2.4	23.229.197.103
Feb 23, 2021 09:00:26.050574064 CET	80	49767	23.229.197.103	192.168.2.4
Feb 23, 2021 09:00:26.050730944 CET	49767	80	192.168.2.4	23.229.197.103
Feb 23, 2021 09:00:26.050930977 CET	49767	80	192.168.2.4	23.229.197.103
Feb 23, 2021 09:00:26.240051985 CET	80	49767	23.229.197.103	192.168.2.4
Feb 23, 2021 09:00:26.258440971 CET	80	49767	23.229.197.103	192.168.2.4
Feb 23, 2021 09:00:26.258481979 CET	80	49767	23.229.197.103	192.168.2.4
Feb 23, 2021 09:00:26.258781910 CET	49767	80	192.168.2.4	23.229.197.103
Feb 23, 2021 09:00:26.258807898 CET	49767	80	192.168.2.4	23.229.197.103
Feb 23, 2021 09:00:26.447956085 CET	80	49767	23.229.197.103	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:58:18.862360001 CET	53723	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:18.898766994 CET	64646	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:18.911287069 CET	53	53723	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:18.947359085 CET	53	64646	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:19.170614958 CET	65298	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:19.219403028 CET	53	65298	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:20.837881088 CET	59123	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:20.886643887 CET	53	59123	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:21.803251982 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:21.854785919 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:22.494116068 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:22.552618027 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:22.623030901 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:22.671576977 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:23.635773897 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:23.687556028 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:24.639569044 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:24.688286066 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:48.091200113 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:48.142822027 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:49.042687893 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:49.099924088 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:49.917707920 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:49.969238997 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:51.016117096 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:51.067745924 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:51.809954882 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:51.858937025 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:52.633148909 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:52.682436943 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:53.913933992 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:53.965698004 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:54.282479048 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:54.334002972 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:54.747322083 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:54.795957088 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:55.957005024 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:56.026484013 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:57.354686975 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:57.406266928 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 08:58:59.442359924 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:58:59.491060972 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:00.320329905 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:00.377401114 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:09.531554937 CET	64078	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:59:09.596590042 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:15.546408892 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:15.595046043 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:23.286400080 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:23.353519917 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:24.241563082 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:24.301482916 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:25.089857101 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:25.173163891 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:25.749360085 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:25.809186935 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:26.346574068 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:26.403739929 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:27.002182961 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:27.021836042 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:27.059883118 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:27.086724043 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:27.706384897 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:27.763459921 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:28.665956974 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:28.736999035 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:29.677529097 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:29.734661102 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:30.280334949 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:30.337259054 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:35.141000032 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:35.201513052 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 08:59:45.485291004 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 08:59:45.687182903 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 09:00:03.621087074 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:00:03.671164989 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 09:00:04.547594070 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:00:04.906436920 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 09:00:05.773307085 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:00:05.838593006 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 09:00:25.798266888 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:00:25.860059977 CET	53	59794	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:59:45.485291004 CET	192.168.2.4	8.8.8.8	0x34c5	Standard query (0)	www.pophazard.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:00:04.547594070 CET	192.168.2.4	8.8.8.8	0xb733	Standard query (0)	www.246835.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:00:25.798266888 CET	192.168.2.4	8.8.8.8	0x8902	Standard query (0)	www.kaieteurny.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:59:45.687182903 CET	8.8.8.8	192.168.2.4	0x34c5	No error (0)	www.pophazard.com		204.11.56.48	A (IP address)	IN (0x0001)
Feb 23, 2021 09:00:04.906436920 CET	8.8.8.8	192.168.2.4	0xb733	No error (0)	www.246835.com	sll.nnu.pw		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:00:04.906436920 CET	8.8.8.8	192.168.2.4	0xb733	No error (0)	sll.nnu.pw		103.66.59.142	A (IP address)	IN (0x0001)
Feb 23, 2021 09:00:25.860059977 CET	8.8.8.8	192.168.2.4	0x8902	No error (0)	www.kaieteurny.com	kaieteurny.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:00:25.860059977 CET	8.8.8.8	192.168.2.4	0x8902	No error (0)	kaieteurny.com		23.229.197.103	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.pophazard.com
- www.246835.com
- www.kaieteurny.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49763	204.11.56.48	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:59:45.858961105 CET	6811	OUT	GET /ntg/?ojoHzZ=ezEzfTUVqdhTeHhhSUO1nROjhCSdyq2ILgetv621tco9QxJ0Ek6h+l0QSU1+LT7ErdbR&1bm=GPD0lNKPfFHTAb HTTP/1.1 Host: www.pophazard.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 08:59:46.287998915 CET	6813	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:59:45 GMT Server: Apache Set-Cookie: vsid=918vr3616127860534399; expires=Sun, 22-Feb-2026 07:59:46 GMT; Max-Age=157680000; path=/; domain=www.pophazard.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_F6FX+ZNnJXLKTmtoz4Zbn33M3dcgDySmD+TZ LM31TPXG44ciXETJu/O4ZJisipBqiF85zsahUw0ArWA/pDFCdw== Keep-Alive: timeout=5, max=112 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 35 62 39 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 70 6f 70 68 61 7a 61 72 64 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 70 6f 70 68 61 7a 61 72 64 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 70 6f 70 68 61 7a 61 72 64 2e 63 6f 6d 2f 73 6b 2d 6c 6f 67 61 62 70 73 74 61 74 75 73 2e 70 68 70 3f 61 3d 61 47 34 32 51 58 64 4c 5a 45 70 78 56 44 52 35 59 32 52 71 4e 55 74 42 62 6e 49 76 61 55 4e 4e 61 57 4a 56 64 45 56 51 56 6a 6c 4a 4d 55 78 56 52 32 64 77 57 46 46 45 53 48 64 4b 56 32 56 6c 61 44 46 33 54 6a 68 30 56 6b 74 6e 5a 45 70 4d 64 6b 52 6c 4b 32 35 47 61 30 52 42 4e 48 46 72 4c 31 64 61 61 55 70 49 4d 54 56 5a 4f 55 31 50 53 30 64 6e 4d 45 31 58 57 6c 6c 36 57 6b 56 6b 52 56 55 78 54 32 39 58 62 48 52 56 53 6c 55 39 26 62 3d 22 2b 61 62 70 3b 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 69 6d 67 6c 6f 67 29 3b 69 66 28 74 79 70 65 6f 66 20 61 62 70 65 72 75 Data Ascii: 5b93<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><script type="text/javascript">var abp;</script><script type="text/javascript" src="http://www.pophazard.com/px.js?ch=1"></script><script type="text/javascript" src="http://www.pophazard.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style.width="0px";imglog.src="http://www.pophazard.com/sk-logabpstatus.php?a=aG42QXdLZEpxVDR5Y2RqNUtBbnIvaUNNaWJVdEVQVjlJMUxVR2dwWFFESHdKV2VlaDF3Tjh0VktnZEpMdkRlK25Ga0RBNHFrL1daaUpIMTVZOU1PS0dnME1XWll6WkVkRVUxT29XbHRVSlU9&b="+abp;document.body.appendChild(imglog);if(typeof abperu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49765	103.66.59.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:00:05.239259958 CET	6841	OUT	GET /ntg/?ojoHzZ=w4X+hAUHJfroJmp94c1onPOAPenZZpTxtRzXhSWsn9e2URXOAMjiMifVYC4X6954J+Dz&1bm=GPD0lNKPfFHTAb HTTP/1.1 Host: www.246835.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:00:05.594891071 CET	6841	IN	HTTP/1.1 302 Found Cache-Control: private Content-Type: text/html; charset=utf-8 Location: https://www.246835.com/ntg/?ojohzz=w4x+hauhjfrojmp94c1onpoapenzzptxtrzxhswsn9e2urxoamjimifvyc4x6954j+dz&1bm=gpd0lnkpffhtab Server: Microsoft-IIS/10.0 X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Date: Tue, 23 Feb 2021 08:00:05 GMT Connection: close Content-Length: 243 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 32 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 32 34 36 38 33 35 2e 63 6f 6d 2f 6e 74 67 2f 3f 6f 6a 6f 68 7a 7a 3d 77 34 78 2b 68 61 75 68 6a 66 72 6f 6a 6d 70 39 34 63 31 6f 6e 70 6f 61 70 65 6e 7a 7a 70 74 78 74 72 7a 78 68 73 77 73 6e Data Ascii: <html><head><title>Object moved</title></head><body><h2>Object moved to <a href="https://www.246835.com/ntg/?ojohzz=w4x+hauhjfrojmp94c1onpoapenzzptxtrzxhswsn

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49767	23.229.197.103	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:00:26.050930977 CET	6853	OUT	GET /ntg/?ojoHzZ=bxqEOtZwpu8QOdqfa5M05y7zdw+lGZ3K+8kzjODwarG6Nc6O9nhCMo5PAGRXJYSnY3HU&1bm=GPD0lNKPfFHTAb HTTP/1.1 Host: www.kaieteurny.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:00:26.258440971 CET	6854	IN	HTTP/1.1 500 Internal Server Error Date: Tue, 23 Feb 2021 08:00:26 GMT Server: Apache Content-Length: 676 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 35 30 30 20 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 73 65 72 76 65 72 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 61 6e 20 69 6e 74 65 72 6e 61 6c 20 65 72 72 6f 72 20 6f 72 0a 6d 69 73 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 61 6e 64 20 77 61 73 20 75 6e 61 62 6c 65 20 74 6f 20 63 6f 6d 70 6c 65 74 65 0a 79 6f 75 72 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 70 3e 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 74 68 65 20 73 65 72 76 65 72 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 61 74 20 0a 20 77 65 62 6d 61 73 74 65 72 40 6b 61 69 65 74 65 75 72 6e 79 2e 63 6c 69 71 75 65 73 2e 63 6f 6d 20 74 6f 20 69 6e 66 6f 72 6d 20 74 68 65 6d 20 6f 66 20 74 68 65 20 74 69 6d 65 20 74 68 69 73 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 2c 0a 20 61 6e 64 20 74 68 65 20 61 63 74 69 6f 6e 73 20 79 6f 75 20 70 65 72 66 6f 72 6d 65 64 20 6a 75 73 74 20 62 65 66 6f 72 65 20 74 68 69 73 20 65 72 72 6f 72 2e 3c 2f 70 3e 0a 3c 70 3e 4d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 61 62 6f 75 74 20 74 68 69 73 20 65 72 72 6f 72 20 6d 61 79 20 62 65 20 61 76 61 69 6c 61 62 6c 65 0a 69 6e 20 74 68 65 20 73 65 72 76 65 72 20 65 72 72 6f 72 20 6c 6f 67 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 35 30 30 20 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>500 Internal Server Error</title></head><body> Internal Server Error The server encountered an internal error ormisconfiguration and was unable to completeyour request. Please contact the server administrator at webmaster@kaieteurny.cliques.com to inform them of the time this error occurred, and the actions you performed just before this error. More information about this error may be availablein the server error log. Additionally, a 500 Internal Server Errorerror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Code Manipulations

User Modules

Hook Summary

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

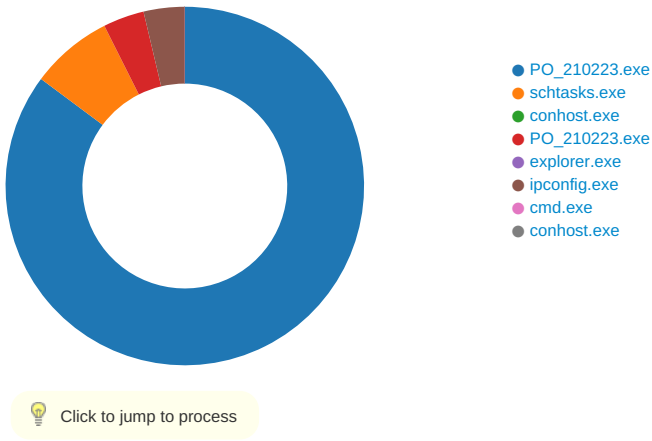
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE6
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE6
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE6
GetMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE6

Statistics

Behavior



System Behavior

Analysis Process: PO_210223.exe PID: 6976 Parent PID: 5920

General

Start time:	08:58:25
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PO_210223.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_210223.exe'
Imagebase:	0x890000
File size:	802304 bytes
MD5 hash:	E40AF9745E938B72D5D860BBC679AEBF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.680445109.0000000002C2D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.681205179.0000000004429000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.681205179.0000000004429000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.681205179.0000000004429000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	unknown
C:\Users\user\AppData\Roaming\kwqifureL.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\kwqifureL.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp33D2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_210223.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp33D2.tmp	success or wait	1	6BFC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kwqifureL.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 88 51 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 2a 0c 00 00 12 00 00 00 00 00 00 ae 49 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Q4`.......... ....P..*...........I... ...`....@.. ....@................	success or wait	4	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\kwqifureL.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp33D2.tmp	unknown	1642	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_210223.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D48C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 1556 Parent PID: 6976

General

Start time:	08:58:39
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kwqifureL' /XML 'C:\Users\user\AppData\Local\Temp\tmp33D2.tmp'
Imagebase:	0xb80000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp33D2.tmp	unknown	2	success or wait	1	B8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp33D2.tmp	unknown	1643	success or wait	1	B8ABD9	ReadFile

Analysis Process: conhost.exe PID: 1744 Parent PID: 1556

General

Start time:	08:58:39
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PO_210223.exe PID: 1868 Parent PID: 6976

General

Start time:	08:58:40
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PO_210223.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO_210223.exe
Imagebase:	0xc30000
File size:	802304 bytes
MD5 hash:	E40AF9745E938B72D5D860BBC679AEBF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.715452206.0000000001180000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.715452206.0000000001180000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.715452206.0000000001180000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.715093547.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.715093547.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.715093547.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.715862611.000000000016B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.715862611.000000000016B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.715862611.000000000016B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E47	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 1868

General

Start time:	08:58:42
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: 6744 Parent PID: 3424

General

Start time:	08:58:56
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0xe50000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
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: 0000000D.00000002.907288680.00000000009B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.907288680.00000000009B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.907288680.00000000009B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.907602619.0000000000D90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.907602619.0000000000D90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.907602619.0000000000D90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.907432455.0000000000C60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.907432455.0000000000C60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.907432455.0000000000C60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	9C9E47	NtReadFile

Analysis Process: cmd.exe PID: 7112 Parent PID: 6744

General

Start time:	08:59:00
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO_210223.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7092 Parent PID: 7112

General

Start time:	08:59:01
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis