ID: 510596
Sample Name:
PO_101&102.exe
Cookbook: default.jbs
Time: 00:21:09
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

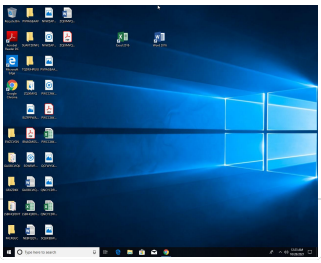
Windows Analysis Report PO_101&102.exe

Overview

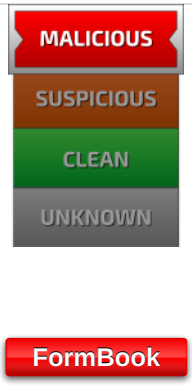
General Information

Sample Name:	PO_101&102.exe
Analysis ID:	510596
MD5:	d814902ba2d06c..
SHA1:	152f01b88a43ae7.
SHA256:	cce115dcfb19503..
Tags:	exe formbook
Infos:	

Most interesting Screenshot:



Detection



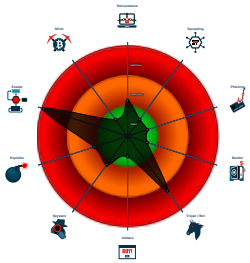
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- PO_101&102.exe (PID: 7068 cmdline: 'C:\Users\user\Desktop\PO_101&102.exe' MD5: D814902BA2D06C94C66F52CE53ED1428)
  - PO_101&102.exe (PID: 6060 cmdline: {path} MD5: D814902BA2D06C94C66F52CE53ED1428)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 6924 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 1496 cmdline: /c del 'C:\Users\user\Desktop\PO_101&102.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.reynbetgirisi.com/snr6/"
  ],
  "decoy": [
    "jjglassmi1.com",
    "vpsseattle.com",
    "drfllc.top",
    "staycoolonline.com",
    "eptlove.com",
    "solusimatasehat.site",
    "ionrarecharlestonproperties.com",
    "b3eflucg.xyz",
    "tvchosun-usa.com",
    "mmahzxwzsadqlshop.life",
    "gospelimport.com",
    "demoapps.website",
    "jackburst54.com",
    "99rocket.education",
    "ccbwithbri.com",
    "trapperairsoft.com",
    "useroadly.com",
    "ralphlaurenonline-nl.com",
    "loanmaster4u.com",
    "champ-beauty-tomigaoka-nail.com",
    "theripemillennial.com",
    "123intan.net",
    "typopendant.com",
    "coruscant.holdings",
    "bio-intelligenz-therapie.com",
    "reprv.com",
    "directreport.net",
    "phinespe.xyz",
    "xuvedae.site",
    "idilikproperties.info",
    "wakigaggenin.com",
    "mal2tech.com",
    "nftwhaler.xyz",
    "gxhnjssx.com",
    "ozba.xyz",
    "lecupcake.net",
    "lucid.quest",
    "kaleoslawncare.com",
    "tiew.store",
    "texcommercialpainting.com",
    "2152351.com",
    "likewize-xl.com",
    "dacooligans.com",
    "manuelmartinezs.com",
    "beancusp.com",
    "barbershopvalleyvillage.com",
    "southwickfunerals.com",
    "briellebaeslay.info",
    "rebeccarye.com",
    "unitedstateswelders.com",
    "saudiarabiavegan.com",
    "testcarona.com",
    "serverapsd.com",
    "crickx.email",
    "hdszbj.com",
    "bennettmountainoutfitter.com",
    "leileilei1999.xyz",
    "baroquefolke.com",
    "francinegeorges.com",
    "horpces.online",
    "resolutionfix.com",
    "mike-schultz.xyz",
    "sohutobankueahomupezinkv.xyz",
    "flowerseedqueen.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.348466397.0000000000FB0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.348466397.0000000000FB0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.348466397.0000000000FB0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000000.333516525.000000000F6F6000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000000.333516525.000000000F6F6000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x21a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x292f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x141c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x992a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.PO_101&102.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.PO_101&102.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.0.PO_101&102.exe.400000.6.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
9.0.PO_101&102.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.PO_101&102.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Yara detected FormBook
- Antivirus detection for URL or domain
- Machine Learning detection for sample

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)
- Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

- Modifies the prolog of user mode functions (user mode inline hooks)
- Self deletion via cmd delete

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)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Injects a PE file into a foreign processes
- 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

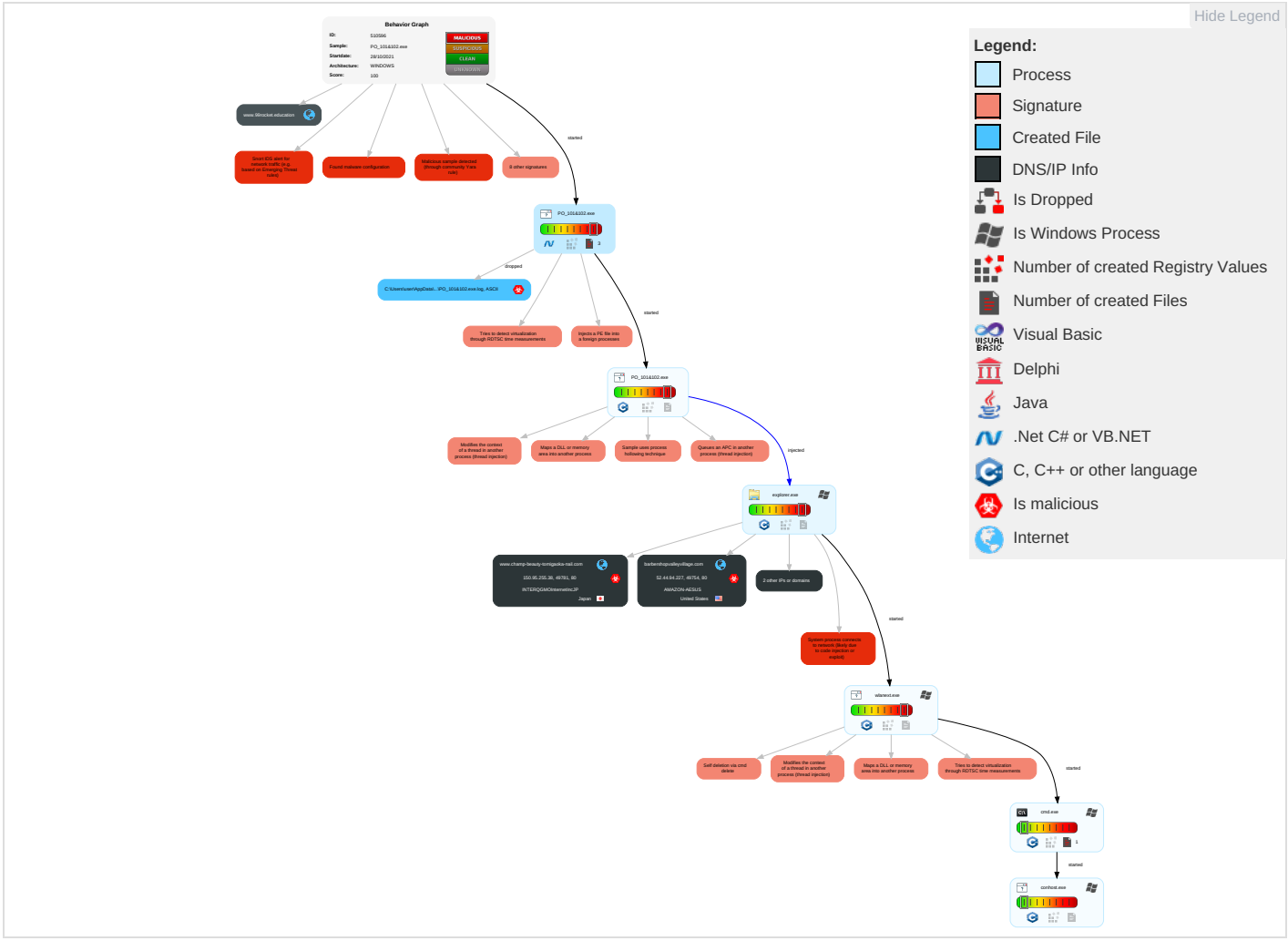
Remote Access Functionality:

Yara detected FormBook

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 Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 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 Communica
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 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

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_101&102.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.PO_101&102.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.PO_101&102.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.PO_101&102.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.PO_101&102.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.barbershopvalleyvillage.com/snr6/?v0DD=Zy5Qpi9o71BxgS1SycsJXGxeSETLIPANxi7ogI8FlHlRlRfybFGNqMyxmIVsIwo4eCM0&p2MTV=Jf94jZD8vHv8m	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
www.reynbetgirisi.com/snr6/	100%	Avira URL Cloud	malware	
http://www.champ-beauty-tomigaoka-nail.com/snr6/?v0DD=AT56xQorg2W9iGq4d7Tt4iWj+Y9aO9Wbdx0aYCn8sjL6tNqdMMFemPCECz3N3nQc4IZ0&p2MTV=Jf94jZD8vHv8m	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://tempuri.org/DatabaseDataSet.xsd	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
barbershopvalleyvillage.com	52.44.94.227	true	true		unknown
www.99rocket.education	208.91.197.39	true	false		unknown
www.champ-beauty-tomigaoka-nail.com	150.95.255.38	true	true		unknown
www.barbershopvalleyvillage.com	unknown	unknown	true		unknown
www.reprv.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.barbershopvalleyvillage.com/snr6/?v0DD=Zy5Qpi9o71BxgS1SycsJXGxeSETLIPANxi7ogI8FlHlRlRfybFGNqMyxmIVsIwo4eCM0&p2MTV=Jf94jZD8vHv8m	true	• Avira URL Cloud: safe	unknown
www.reynbetgirisi.com/snr6/	true	• Avira URL Cloud: malware	low
http://www.champ-beauty-tomigaoka-nail.com/snr6/?v0DD=AT56xQorg2W9iGq4d7Tt4iWj+Y9aO9Wbdx0aYCn8sjL6tNqdMMFemPCECz3N3nQc4IZ0&p2MTV=Jf94jZD8vHv8m	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.44.94.227	barbershopvalleyvillage.com	United States		14618	AMAZON-AESUS	true
150.95.255.38	www.champ-beauty-tomigaoka-nail.com	Japan		7506	INTERQGMOInternetIncJP	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510596
Start date:	28.10.2021
Start time:	00:21:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO_101&102.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:	25
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@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.1% (good quality ratio 16.2%) • Quality average: 73% • Quality standard deviation: 31.5%
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

Time	Type	Description
00:22:03	API Interceptor	2x Sleep call for process: PO_101&102.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.44.94.227	Ohki Blower Skid Base Enquiry 052521.exe	Get hash	malicious	Browse	• www.lawndaleballoons.com/un8c/?5j9=e1aIhBu54HwvDa9jIFoPTn+x8qwz6+WyuS6TAcXGUJ0TuA7XqmfqjA7rvtpmBfuRBanb&vR=Ltxx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.accokeektvmounting.com/eao/?xb08qf=FCtAuHshdr0f2dc4fuyEfDsgR0BafKiFq6O5QuD89NG0N45OyG6nKW+GSjtGDGmhuPTR&1bz=xpn0PfXxSXAtfZap
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• www.accokeektvmounting.com/eao/?Yvux40tX=FCtAuHshdr0f2dc4fuyEfDsgR0BafKiFq6O5QuD89NG0N45OyG6nKW+GSjtsc2WhqNbR&Pp=jfLprdxxs
150.95.255.38	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• www.e-readertnpasumo5.xyz/mwev/?n8o8k4=s6JjqHrQhtmRWbO5qNja442Ngbg13E4gPlYXf4CDaMRBDRGw8TbY6EH4VHnxd8/K7vvQVg==&ap=-Zj4
	F30AGnBthja6Ka2.exe	Get hash	malicious	Browse	• www.lm-safe-keepingtoyof4.xyz/n35q/?g6YDq=Wv0dqvs8lJwXid_P&5joLT4Q=IZFN/VIywbhLRJtRnBeGYuVozig+PLM9162SZrHwuJmr7rD0xTfdi4jzZlcOLsRTbY5a
	Diagram and Specifications.exe	Get hash	malicious	Browse	• www.lly03toyof4.xyz/sw39/?3fl0hDv=H19d1GjxiY7aDYQouKVpvu5ugVR3f0gotfGKpnd7ufTQ/ckXv8DnpDWqGu8YbIlnhBEC&hL=4hu4Zrlx
	soa_02010021.exe	Get hash	malicious	Browse	• www.eco1tnpasumo3.xyz/nqn4/?rN64X=Mv6pP6pP&-ZddGje=vanPYQUuZ3XFRC7SYcRcV+oaGEE9ir47lHLJmRrDHNXTaYXBSumhPRu6vgIi5Ucq3YEQ
	AWB-kp035Maersk.exe	Get hash	malicious	Browse	• www.lightswaranwgt76.xyz/cl8k/?l8PHbJ2P=7o17KyM4PBNcdnCS5DRkZ/XJrfTNVAQ49VkyourTKnWaeF8IIwoMfqHFOrhZgIdgF0AK&7nnp_=AV0l

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MV ROCKET_PDA.exe	Get hash	malicious	Browse	• www.eco1tnpasumo3.xyz/nqn4/?T2MpwT=vanPYQUuZ3XFRC7SYcRcV+oaGEE9ir47lHLJmRrDHNXTaYXBSumhPRu6vjoy21MSp9tX&VDK0L=5jZhjDchE
	n14Gz5Qjcb.exe	Get hash	malicious	Browse	• www.rawhoneytnpasumo6.xyz/m0np/?9rjPn6YP=jlbGx/ze8CP5AGcSSAWWd1mzA5QWN95ANb9dADdfV40QuflaaY29PF8tVyxQyxmkQaSl&j6782P=EZM4Hn6
	SYsObQNkC1.exe	Get hash	malicious	Browse	• www.rawhoneytnpasumo6.xyz/m0np/?U2Jprb-=jlbGx/ze8CP5AGcSSAWWd1mzA5QWN95ANb9dADdfV40QuflaaY29PF8tVxRA9Q2cO/7P&cT=7nBDtz4x
	SALES CONTRACT 914 VIPA ORDER 213581.xlsx	Get hash	malicious	Browse	• www.yozotnpasumo4.xyz/9gdg/?n8JX4=rhbOZ5tChQo7vrxyCoT/NvoAZwtLS/ySMYcbtm1mQnSdzkl9qiVaOt/asz9lxM02ycbsgg==&e6AX=9rIPB
	EIElnDxX0V.exe	Get hash	malicious	Browse	• www.rawhoneytnpasumo6.xyz/m0np/?5joLnT=jlbGx/ze8CP5AGcSSAWWd1mzA5QWN95ANb9dADdfV40QuflaaY29PF8tVy9QhhqnJKSer7wyaw==&x48L=9rPL8fGx8
	DOC.exe	Get hash	malicious	Browse	• www.businesszukai.com/imm8/?oZBd28E8=FtzG4nVao7RGnpiPAUTOHzX+ComCJgTxVAA7jEIQ99qrgC2i4yGXxLE7fpRdiVaJ0w+u&7n6hj=p2MtFfu8w4Y

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PAYMENT ADVISE CONFIRMATION.xlsx	Get hash	malicious	Browse	• www.rjb355.xyz/att3/?d8EdM=5jeDV20pBRJHXPo0&AHRDZVs=bhDRCC3Yl61/258JNgDxkJaKmIOd6kTln+2NX7EMzgyYOep5PphbUdqUvSZC+n+eFvYVMg==
	PROFOMA INVOICE NO2021TD24 PDF.exe	Get hash	malicious	Browse	• www.hold-sometimes.xyz/ssee/?MBZp=A0DTKVI&k0GDpTe=SLXqLbVogVOmzD5x7TF5YDBiNFFEDQhqQaeiGgch4Tvb9L/HBk+4drk9DekX4BUJHdpE
	#7091.pdf.exe	Get hash	malicious	Browse	• www.gwh525.xyz/gm9w/?kZR=SBgXj&5j=pl70zmZe6iC967JcRkVJi5bANyE1hTx+7JFuE+QWvqw/ndgwpf2/G4CCDYTbrIzzAG/c
	RFQ, Scope of Requirements PDF.exe	Get hash	malicious	Browse	• www.hold-sometimes.xyz/ssee/?c6A8szA=SLXqLbVogVOmzD5x7TF5YDBiNFFEDQhqQaeiGgch4Tvb9L/HBk+4drk9Dek9nxkJDfhE&ZRqLPd=7nE0dtjpKd7
	Order_2084.exe	Get hash	malicious	Browse	• www.somethingwild.com/rqe8/?oZhtNxR=QYiwiO9SCZDy/G7W+Bo397AAf+TAkPtFsK9VX0BihvC7Ep5smT5MjlmXlwucRZfhSaQc&7n=h40X
	Pending DHL Shipment Notification REF 81621.exe	Get hash	malicious	Browse	• www.hold-sometimes.xyz/ssee/?-ZeDzN_=SLXqLbVogVOmzD5x7TF5YDBiNFFEDQhqQaeiGgch4Tvb9L/HBk+4drk9DekX4BUJHdpE&xJBTI=PHsdF4OxqDN8N8ZP
	hu3fkyvz5Y.exe	Get hash	malicious	Browse	• www.o72lab.com/i7dg/?A6AT=KLqFW7q7vJQ5dEUL0c1bE2IQuFF8GNWa2S5pk1tOJ4HLfTR1kNQ1OKxzY4oES7RxnevF&knZ=1by0_ZBPIXv80F

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Remittance.exe	Get hash	malicious	Browse	• www.oneonecity.xyz/udew/?5jS0E=y0DP&fZ=N+HvIhXSEX4Ftk11NAt0NiYU1gvcyzQfzCwODxtCZBlrbwkU/Fmy7dLNUhQJfDmEovY5
	PI_NGOIU00987.exe	Get hash	malicious	Browse	• www.alexgoestech.xyz/uecu/?KJE0k=v3ox63M4CDEHY+dz4sl2sSOFGFYDWtyb6TlC+A0rVG3GBM4V/JHpU4VTMu4TbGy/jm8X&7n=MDKTHlx8Z

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INTERQGMOInternetIncJP	CtTYTpaAKA.exe	Get hash	malicious	Browse	• 157.7.107.193
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 150.95.255.38
	F9ObnUc4ol.exe	Get hash	malicious	Browse	• 118.27.122.187
	DHL_119040 receipt document,pdf.exe	Get hash	malicious	Browse	• 150.95.219.218
	n7gjtO4ZwD.exe	Get hash	malicious	Browse	• 118.27.122.92
	F30AGnBthja6Ka2.exe	Get hash	malicious	Browse	• 150.95.255.38
	PFD33mzc5l	Get hash	malicious	Browse	• 118.27.80.204
	comingback.exe	Get hash	malicious	Browse	• 118.27.122.217
	MV ANACAPA LIGHT.xlsx	Get hash	malicious	Browse	• 118.27.122.214
	cyberantix-PayroLL-997263-pdf.HtML	Get hash	malicious	Browse	• 150.95.219.148
	cyberantix-PayroLL-997263-pdf.HtML	Get hash	malicious	Browse	• 150.95.219.148
	8jfOcvTqQA	Get hash	malicious	Browse	• 163.44.189.209
	IN7REq0Jv5	Get hash	malicious	Browse	• 133.130.112.119
	GDs-#09283 DIAGRAM AND PRODUCT SPECIFICATIONS.pdl.exe	Get hash	malicious	Browse	• 150.95.59.10
	s0bi9t	Get hash	malicious	Browse	• 210.157.44.132
	Diagram and Specifications.exe	Get hash	malicious	Browse	• 150.95.255.38
	soa_02010021.exe	Get hash	malicious	Browse	• 150.95.255.38
	sLtLgOtoPA.exe	Get hash	malicious	Browse	• 157.7.107.193
	94VG.arm	Get hash	malicious	Browse	• 157.7.100.11
	PO08485.xlsx	Get hash	malicious	Browse	• 118.27.122.218
AMAZON-AESUS	UW_230 West 41st St_20211027.xlsm	Get hash	malicious	Browse	• 52.204.158.151
	e6dff8475541ebddc1f0db47a311eb2c25581b7d5e62a.exe	Get hash	malicious	Browse	• 3.209.18.1
	arm7	Get hash	malicious	Browse	• 23.21.163.253
	x86_64	Get hash	malicious	Browse	• 52.86.141.255
	Purchase order.doc	Get hash	malicious	Browse	• 54.156.84.168
	triage_dropped_file.dll	Get hash	malicious	Browse	• 3.232.242.170
	Payment Advice.exe	Get hash	malicious	Browse	• 3.223.115.185
	AWB#708900271021,PDF.exe	Get hash	malicious	Browse	• 34.237.7.9
	2jFfKOEefN.exe	Get hash	malicious	Browse	• 3.223.115.185
	vx55dc0wlv.exe	Get hash	malicious	Browse	• 34.233.132.165
	SKGCM_YAHYA AZHEBS#U0130 Ponuda proizvoda7.exe	Get hash	malicious	Browse	• 52.20.84.62
	usuyeoiSVT.exe	Get hash	malicious	Browse	• 44.199.40.234
	PLSW217DEJ59.vbs	Get hash	malicious	Browse	• 34.199.8.144
	Order.exe	Get hash	malicious	Browse	• 3.223.115.185
	RIVERSEDGE #PO, INVOICE Acknowledge & E- Check Remittance Advice - Copy.html	Get hash	malicious	Browse	• 35.168.68.183
	payment advice_16000.exe	Get hash	malicious	Browse	• 52.21.5.29
	hSNPFOpBGX.exe	Get hash	malicious	Browse	• 3.220.57.224
	Wq9FLAFuS8.exe	Get hash	malicious	Browse	• 54.91.6.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Unpaid invoice.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMS211323.xlsx	Get hash	malicious	Browse	• 54.192.66.129

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_101&102.exe.log

Process:	C:\Users\user\Desktop\PO_101&102.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.424831742558016
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO_101&102.exe
File size:	680960
MD5:	d814902ba2d06c94c66f52ce53ed1428
SHA1:	152f01b88a43ae7f0cf486a947bb0b0b23496827
SHA256:	cce115dcfb19503dfbc71566681425094ca56887fc1afe85b9bc9788341312bf
SHA512:	ea59a8d6d27b1434ae2245c8d708a1a94f066721de015c3a8d40af55fdcbf98e71a8af9e3006bda6874444ca9fee79f5338ace935392b5cba5d02b2a2ce956dd
SSDEEP:	12288:JVMVrsFuujDwb/UH4Z5dH4ien5nh623Rl6rxIeSRobTmWDhLsqJFTP:JKVrsFuuj+UH4Z5qignFD2lwWdQq

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...~.ya.....P..Z.....y... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a79ee
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:	0x6179BF7E [Wed Oct 27 21:07:10 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa59f4	0xa5a00	False	0.697439563679	data	7.43356279731	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x5a4	0x600	False	0.41796875	data	4.0566993219	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/28/21-00:23:09.142294	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	52.44.94.227
10/28/21-00:23:09.142294	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	52.44.94.227

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/28/21-00:23:09.142294	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	52.44.94.227

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 00:23:08.112143993 CEST	192.168.2.3	8.8.8.8	0x9e4c	Standard query (0)	www.barbershopvalleyvillage.com	A (IP address)	IN (0x0001)
Oct 28, 2021 00:23:25.489010096 CEST	192.168.2.3	8.8.8.8	0x9a2	Standard query (0)	www.reprv.com	A (IP address)	IN (0x0001)
Oct 28, 2021 00:23:45.706701994 CEST	192.168.2.3	8.8.8.8	0xf2a4	Standard query (0)	www.champ-beauty-tomigaoka-nail.com	A (IP address)	IN (0x0001)
Oct 28, 2021 00:24:07.353573084 CEST	192.168.2.3	8.8.8.8	0x5fea	Standard query (0)	www.99rocket.education	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 00:23:08.136106014 CEST	8.8.8.8	192.168.2.3	0x9e4c	No error (0)	www.barbershopvalleyvillage.com	barbershopvalleyvillage.com		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 00:23:08.136106014 CEST	8.8.8.8	192.168.2.3	0x9e4c	No error (0)	barbershopvalleyvillage.com		52.44.94.227	A (IP address)	IN (0x0001)
Oct 28, 2021 00:23:25.526612043 CEST	8.8.8.8	192.168.2.3	0x9a2	Name error (3)	www.reprv.com	none	none	A (IP address)	IN (0x0001)
Oct 28, 2021 00:23:45.963149071 CEST	8.8.8.8	192.168.2.3	0xf2a4	No error (0)	www.champ-beauty-tomigaoka-nail.com		150.95.255.38	A (IP address)	IN (0x0001)
Oct 28, 2021 00:24:07.479249001 CEST	8.8.8.8	192.168.2.3	0x5fea	No error (0)	www.99rocket.education		208.91.197.39	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.barbershopvalleyvillage.com
- www.champ-beauty-tomigaoka-nail.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49754	52.44.94.227	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 00:23:09.142293930 CEST	5180	OUT	GET /snr6/?v0DD=Zy5Qpi9o71BxgS1SycsJXGxeSETLIPANxi7ogI8FlHlRlRfybFGNqMyxmIVsIwo4eCM0&p2MTV=Jf94jZD8vHv8m HTTP/1.1 Host: www.barbershopvalleyvillage.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 00:23:09.281163931 CEST	5180	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Wed, 27 Oct 2021 22:23:09 GMT Content-Type: text/html Content-Length: 182 Connection: close Location: https://www.barbershopvalleyvillage.com/snr6/?v0DD=Zy5Qpi9o71BxgS1SycsJXGxeSETLIPANxi7ogI8FlHlRlRfybFGNqMyxmIVsIwo4eCM0&p2MTV=Jf94jZD8vHv8m Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 6f 70 65 6e 72 65 73 74 79 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>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49781	150.95.255.38	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 00:23:46.242897034 CEST	5990	OUT	GET /snr6/?v0DD=AT56xQorg2W9iGq4d7Tt4iWj+Y9aO9Wbdx0aYCn8sjL6tNqdMMFemPCECz3N3nQc4IZ0&p2MTV=Jf94jZD8vHv8m HTTP/1.1 Host: www.champ-beauty-tomigaoka-nail.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 28, 2021 00:23:46.519165993 CEST	5991	IN	HTTP/1.1 302 Found Date: Wed, 27 Oct 2021 22:23:46 GMT Server: Apache Location: http://dfltweb1.onamae.com Content-Length: 210 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 32 20 46 6f 75 6e 64 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 46 6f 75 6e 64 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 3a 2f 2f 64 66 6c 74 77 65 62 31 2e 6f 6e 61 6d 61 65 2e 63 6f 6d 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>302 Found</title></head><body> Found The document has moved here. </body></html>

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PO_101&102.exe PID: 7068 Parent PID: 5480

General

Start time:	00:21:56
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\PO_101&102.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_101&102.exe'
Imagebase:	0x530000
File size:	680960 bytes
MD5 hash:	D814902BA2D06C94C66F52CE53ED1428
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: 00000001.00000002.294755714.00000000039A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.294755714.00000000039A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.294755714.00000000039A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: PO_101&102.exe PID: 6060 Parent PID: 7068

General

Start time:	00:22:04
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\PO_101&102.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x640000
File size:	680960 bytes
MD5 hash:	D814902BA2D06C94C66F52CE53ED1428
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.348466397.0000000000FB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.348466397.0000000000FB0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.348466397.0000000000FB0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.348384221.0000000000D70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.348384221.0000000000D70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.348384221.0000000000D70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.291465505.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.291465505.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.291465505.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.348134923.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.348134923.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.348134923.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.291860367.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.291860367.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.291860367.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 6060

General

Start time:	00:22:07
Start date:	28/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.333516525.000000000F6F6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.333516525.000000000F6F6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.333516525.000000000F6F6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.320955277.000000000F6F6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.320955277.000000000F6F6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.320955277.000000000F6F6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: wlanext.exe PID: 6924 Parent PID: 3352

General

Start time:	00:22:28
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x920000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.542137974.0000000003070000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.542137974.0000000003070000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.542137974.0000000003070000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.539322069.00000000008D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.539322069.00000000008D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.539322069.00000000008D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.542399139.00000000030A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.542399139.00000000030A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.542399139.00000000030A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1496 Parent PID: 6924

General

Start time:	00:22:33
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO_101&102.exe'
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4008 Parent PID: 1496

General

Start time:	00:22:34
Start date:	28/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis