ID: 452542
Sample Name: PI-0387991.exe
Cookbook: default.jbs
Time: 15:03:58
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

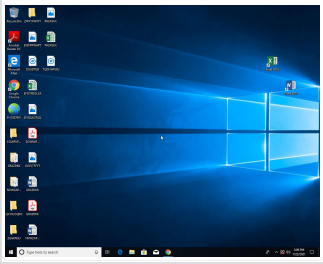
Windows Analysis Report PI-0387991.exe

Overview

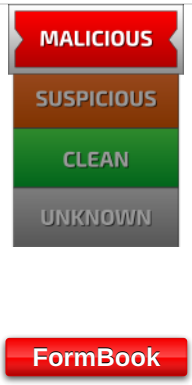
General Information

Sample Name:	PI-0387991.exe
Analysis ID:	452542
MD5:	655318bec9b30d..
SHA1:	23f37c9bddcd839..
SHA256:	8cd1a5c6360cc1…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



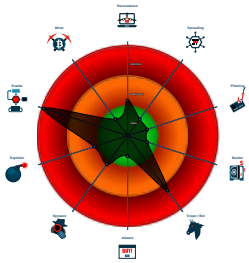
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- PI-0387991.exe (PID: 5736 cmdline: 'C:\Users\user\Desktop\PI-0387991.exe' MD5: 655318BEC9B30D5A2F2DEDF399D87438)
  - RegSvcs.exe (PID: 3328 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 5076 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 4860 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bodymoisturizer.online/q4kr/"
  ],
  "decoy": [
    "realmodapk.com",
    "hanoharuka.com",
    "shivalikspiritualproducts.com",
    "womenshealthclinincagra.com",
    "racketpark.com",
    "startuporig.com",
    "azkachinas.com",
    "klanblog.com",
    "linuxradio.tools",
    "siteoficial-liquida.com",
    "glsbuyer.com",
    "bestdeez.com",
    "teens2cash.com",
    "valleyviewconstruct.com",
    "myfortniteskins.com",
    "cambecare.com",
    "csec2011.com",
    "idookap.com",
    "warmwallsrecords.com",
    "smartmirror.one",
    "alertreels.com",
    "oiop.online",
    "61cratoslot.com",
    "hispanicassoclv.com",
    "pennyforyourprep.com",
    "fayansistanbul.com",
    "superbartendergigs.club",
    "herr-nourimann.com",
    "oatkc.net",
    "romahony.com",
    "sportcrea.com",
    "crystalnieblas.com",
    "lcmet.com",
    "nwaymyatthu-mm.com",
    "edsufferen.club",
    "apispotlight.com",
    "shadowcatrecording.com",
    "capwisefin.com",
    "themesinsider.com",
    "kadrisells.com",
    "db-82.com",
    "rentyoursubmarine.com",
    "rin-ronshop.com",
    "donzfamilia.com",
    "loyalcollegeofart.com",
    "socialize.site",
    "shadesailstructure.com",
    "smcenterbiz.com",
    "zcdonghua.com",
    "1420radiolider.com",
    "ckenpo.com",
    "trucksitasa.com",
    "getthistle.com",
    "usvisanicaragua.com",
    "josiemaxwrites.com",
    "dehaagennutraceuticals.com",
    "noiaapp.com",
    "blinbins.com",
    "getreitive.com",
    "turmericbar.com",
    "manifestwealthrightnow.com",
    "garagekuhn.com",
    "longviewfinancialadvisor.com",
    "hallworthcapital.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.322811703.0000000004381000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.322811703.0000000004381000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xe8af0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xe8e8a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x10ff10:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1102aa:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xf4b9d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x11bfbd:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xf4689:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x11baa9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xf4c9f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x11c0bf:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xf4e17:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x11c237:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xe98a2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x110cc2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xf3904:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x11ad24:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xea61a:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x111a3a:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xf9c8f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1210af:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xfad32:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.322811703.0000000004381000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xf6bc1:$sqlite3step: 68 34 1C 7B E1 • 0xf6cd4:$sqlite3step: 68 34 1C 7B E1 • 0x11dfe1:$sqlite3step: 68 34 1C 7B E1 • 0x11e0f4:$sqlite3step: 68 34 1C 7B E1 • 0xf6bf0:$sqlite3text: 68 38 2A 90 C5 • 0xf6d15:$sqlite3text: 68 38 2A 90 C5 • 0x11e010:$sqlite3text: 68 38 2A 90 C5 • 0x11e135:$sqlite3text: 68 38 2A 90 C5 • 0xf6c03:$sqlite3blob: 68 53 D8 7F 8C • 0xf6d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x11e023:$sqlite3blob: 68 53 D8 7F 8C • 0x11e14b:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.497338116.0000000003390000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.497338116.0000000003390000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.2.RegSvcs.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
8.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
8.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

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)

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

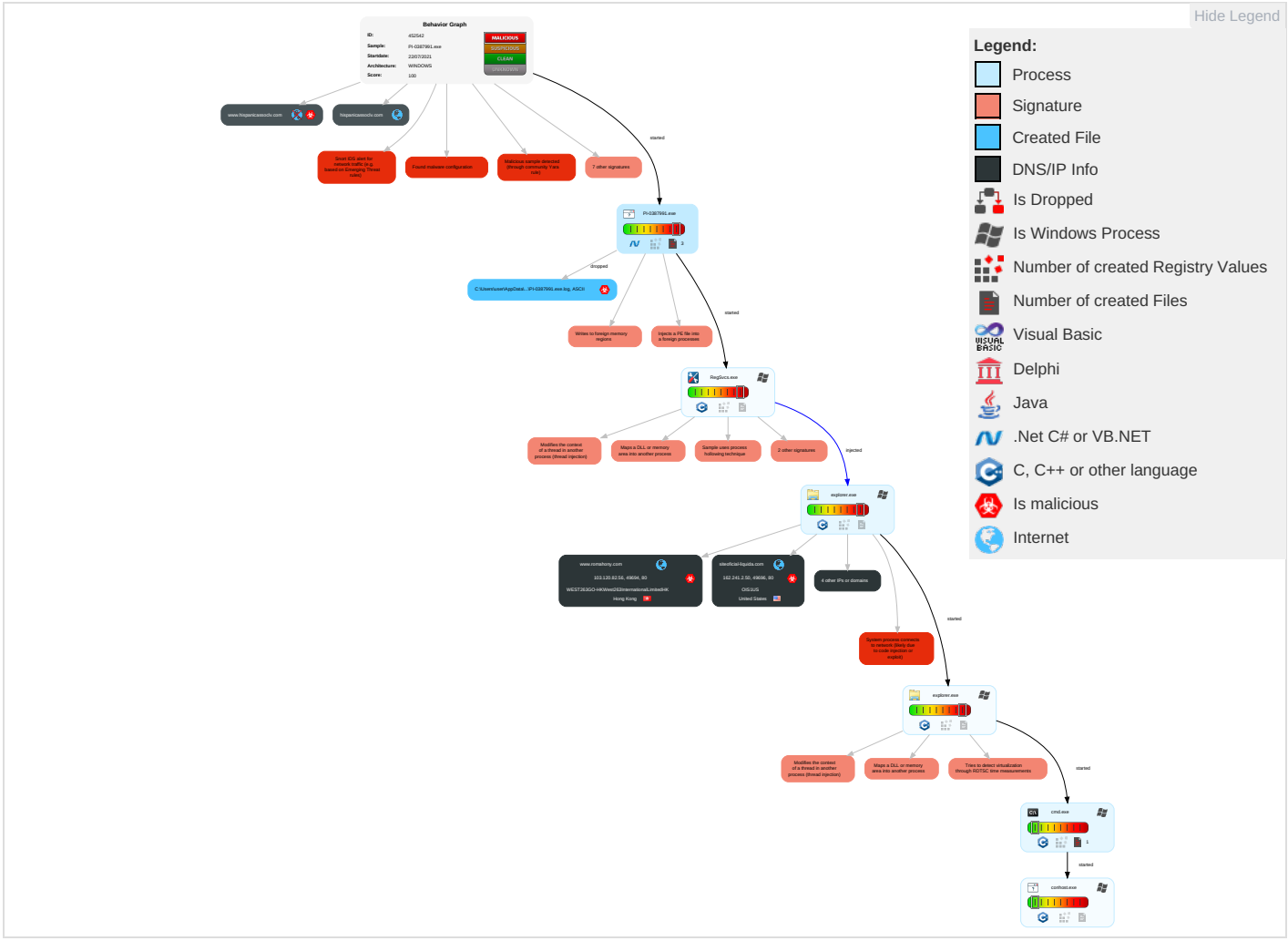
Remote Access Functionality:

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 7 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 7 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	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	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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
PI-0387991.exe	50%	Virustotal		Browse
PI-0387991.exe	43%	ReversingLabs	Win32.Trojan.AgentTesla	
PI-0387991.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RegSvcs.exe.3050000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.explorer.exe.f20000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.0.explorer.exe.f20000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
hispanicassoclv.com	2%	Virustotal		Browse
www.romahony.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
siteoficial-liquida.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.hispanicassoclv.com/q4kr/?m4z=hZWT6D&KdPxHVdh=+adpk/1z85ABQgFM8KoV7nh2RN9wNRyN3NacL4PKZthW2WB1UYKLVSKaUBe2HmITnYf8	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn-i-d)	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/7	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm3	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oil	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.romahony.com/q4kr/?m4z=hZWT6D&KdPxHVdh=stDcKtJiFThdGrRpndYyQbsbrCSX1QkCWnDTnTci+riMDIV/FP53rWURHHZjowo3ayyv	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnobt	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.siteoficial-liquida.com/q4kr/?KdPxHVdh=UTB9cmVppYOj/UC3W28IAi1vRKY7uisBtiUczDixbM3KLxocs5bu1DNZcq72D06e9ENr&m4z=hZWT6D	0%	Avira URL Cloud	safe	
http://www.carterandcone.comporFxlei	0%	Avira URL Cloud	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.sajatypeworks.comx	0%	Avira URL Cloud	safe	
http://www.idookap.com/q4kr/?m4z=hZWT6D&KdPxHVdh=8Twh4s36gZRno0YiIaK1Aog0Jq5SRxj1tGC/kNtcN6cj6UbdIOqmSeR7M7wA7kAlsS0+	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.tiro.com~	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
www.bodymoisturizer.online/q4kr/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/)	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.com_f	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	
http://www.carterandcone.comUfee	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/k-e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hispanicassoclv.com	34.102.136.180	true	false	• 2%, Virustotal, Browse	unknown
www.romahony.com	103.120.82.56	true	true	• 0%, Virustotal, Browse	unknown
siteoficial-liquida.com	162.241.2.50	true	true	• 0%, Virustotal, Browse	unknown
idookap.com	34.102.136.180	true	false		unknown
www.siteoficial-liquida.com	unknown	unknown	true		unknown
www.idookap.com	unknown	unknown	true		unknown
www.bodymoisturizer.online	unknown	unknown	true		unknown
www.hispanicassoclv.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.hispanicassoclv.com/q4kr/?m4z=hZWT6D&KdPxHVdh=+adpk/1z85ABQgFM8KoV7nh2RN9wNRyN3NacL4PKZthW2WB1UYKLVSKaUBe2HmITnYf8	false	• Avira URL Cloud: safe	unknown
http://www.romahony.com/q4kr/?m4z=hZWT6D&KdPxHVdh=stDcKtJiFThdGrRpndYyQbsbrCSX1QkCWnDTnTci+riMDIV/FP53rWURHHZjowo3ayyv	true	• Avira URL Cloud: safe	unknown
http://www.siteoficial-liquida.com/q4kr/?KdPxHVdh=UTB9cmVppYOj/UC3W28IAi1vRKY7uisBtiUczDixbM3KLxocs5bu1DNZcq72D06e9ENr&m4z=hZWT6D	true	• Avira URL Cloud: safe	unknown
http://www.idookap.com/q4kr/?m4z=hZWT6D&KdPxHVdh=8Twh4s36gZRno0YiIaK1Aog0Jq5SRxj1tGC/kNtcN6cj6UbdIOqmSeR7M7wA7kAlsS0+	false	• Avira URL Cloud: safe	unknown
www.bodymoisturizer.online/q4kr/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.120.82.56	www.romahony.com	Hong Kong		139021	WEST263GO-HKWest263InternationalLimitedHK	true
34.102.136.180	hispanicassoclv.com	United States		15169	GOOGLEUS	false
162.241.2.50	siteoficial-liquida.com	United States		26337	OIS1US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452542
Start date:	22.07.2021
Start time:	15:03:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI-0387991.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:	14
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@7/1@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.2% (good quality ratio 29.6%) • Quality average: 71.3% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.120.82.56	MX-M502N_201145.exe	Get hash	malicious	Browse	• www.romahony.com/q4kr/?f48lqdCh=stDcKtJiFThdGrRpndYyQbsbrCSX1QkCWnDTnTci+riMDIV/FP53rWURHE5Z4hlPAVTo&6lE=bN9T
	Fegvc0Wetr.exe	Get hash	malicious	Browse	• www.gcbsclubc.com/nff/?7nz0W=/2QoJkj6lESZa4CqvOXsKAmeRzxfPdS9w4+MBqjVvCLWAIbbuF0NQEAKVb+NJ2vn791v&kT6=Ulg8GPkP8Zgp
	Payment_Advice.exe	Get hash	malicious	Browse	• www.romahony.com/q4kr/?iTntSV=stDcKtJiFThdGrRpndYyQbsbrCSX1QkCWnDTnTci+riMDIV/FP53rWURHHVj7gk0Diy5BlTIew==&5jo=6leTzTsHNnB4
	88DUknYBXu.exe	Get hash	malicious	Browse	• www.gcbsclubc.com/nff/?_JE=/2QoJkj6lESZa4CqvOXsKAmeRzxfPdS9w4+MBqjVvCLWAIbbuF0NQEAKVYe3ZnPfhaUo&-ZkH=9rmDvr4Hp4stJhM

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.2.50	Payment_Swift00987.exe	Get hash	malicious	Browse	• www.siteoficial-liquida.com/q4kr/?9rn0l=6lThAhBX_TDlt&b2Jd2=UTB9cmVppYOj/UC3W28IAi1vRKY7uisBtiUczDixbM3KLxocs5bu1DNZcq32Qk2dkUN92Swnyw==
	Payment_Advice.exe	Get hash	malicious	Browse	• www.siteoficial-liquida.com/q4kr/?iTntSV=UTB9cmVppYOj/UC3W28lAi1vRKY7uisBtiUczDixbM3KLxocs5bu1DNZcq32Qk2dkUN92Swnyw==&5jo=6leTzTsHNnB4
	Payment_Advice.exe	Get hash	malicious	Browse	• www.siteoficial-liquida.com/q4kr/?QtRl=UTB9cmVppYOj/UC3W28lAi1vRKY7uisBtiUczDixbM3KLxocs5bu1DNZcpbmMVqmjhks&w2MLb=6lux

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.romahony.com	MX-M502N_201145.exe	Get hash	malicious	Browse	• 103.120.82.56
	Payment_Advice.exe	Get hash	malicious	Browse	• 103.120.82.56

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEST263GO-HKWest263InternationalLimitedHK	Inv_7623980.exe	Get hash	malicious	Browse	• 103.139.0.9
	fLtlowdmEG.exe	Get hash	malicious	Browse	• 103.139.0.9
	u5xgJUljfl.exe	Get hash	malicious	Browse	• 103.139.0.9
	wininit(1).exe	Get hash	malicious	Browse	• 103.139.0.9
	pedido pdf.exe	Get hash	malicious	Browse	• 219.234.31.177
	MX-M502N_201145.exe	Get hash	malicious	Browse	• 103.120.82.56
	Fegvc0Wetr.exe	Get hash	malicious	Browse	• 103.120.82.56
	Payment_Advice.exe	Get hash	malicious	Browse	• 103.120.82.56
	PO#006611.doc.exe	Get hash	malicious	Browse	• 103.43.188.130
	88DUknYBXu.exe	Get hash	malicious	Browse	• 103.120.82.56
	SHIPPING DOCUMENT_7048555233PDF.exe	Get hash	malicious	Browse	• 103.108.192.24
	Payment Advice-Pdf.exe	Get hash	malicious	Browse	• 103.139.0.9
	Pdf Scen Invoice 17INV06003.exe	Get hash	malicious	Browse	• 103.108.192.24
	PO1234EFJL_011LM000_pdf.exe	Get hash	malicious	Browse	• 219.234.31.216
	REQUEST FOR QUOTATION 1307-RFQ.pdf.exe	Get hash	malicious	Browse	• 43.224.155.141
	TT COPY (39.750,00 USD).exe	Get hash	malicious	Browse	• 103.120.83.153
	ntpxrxZCfL.exe	Get hash	malicious	Browse	• 218.247.86.90
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 218.247.86.90
	Shipping Doc.exe	Get hash	malicious	Browse	• 219.234.8.81
	Client.vbs	Get hash	malicious	Browse	• 103.120.80.6
OIS1US	vGXbKUQZZpb0fE8.exe	Get hash	malicious	Browse	• 162.241.85.193
	K7EnL0C9KJ.exe	Get hash	malicious	Browse	• 192.185.147.20
	Gift Card 0796907.xlsb	Get hash	malicious	Browse	• 162.241.3.29
	Gift Card 0796907.xlsb	Get hash	malicious	Browse	• 162.241.3.29
	Order 9572478.xlsb	Get hash	malicious	Browse	• 162.241.2.50
	Order 9572478.xlsb	Get hash	malicious	Browse	• 162.241.2.50
	Order 161488.xlsb	Get hash	malicious	Browse	• 162.241.3.14

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 491196.xlsb	Get hash	malicious	Browse	• 50.116.94.238
	Order 161488.xlsb	Get hash	malicious	Browse	• 162.241.3.14
	PO 491196.xlsb	Get hash	malicious	Browse	• 50.116.94.238
	Order 46975986.xlsb	Get hash	malicious	Browse	• 162.241.3.29
	WO 2308349.xlsb	Get hash	malicious	Browse	• 162.241.2.147
	Order 46975986.xlsb	Get hash	malicious	Browse	• 162.241.3.29
	WO 2308349.xlsb	Get hash	malicious	Browse	• 162.241.2.147
	PO 0314935.xlsb	Get hash	malicious	Browse	• 162.241.3.29
	WO 2825876.xlsb	Get hash	malicious	Browse	• 162.241.3.14
	PO 0314935.xlsb	Get hash	malicious	Browse	• 162.241.3.29
	WO 2825876.xlsb	Get hash	malicious	Browse	• 162.241.3.14
	Order 1744163.xlsb	Get hash	malicious	Browse	• 50.116.94.238
	statistic-1496367785.xls	Get hash	malicious	Browse	• 162.241.2.112

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI-0387991.exe.log	
Process:	C:\Users\user\Desktop\PI-0387991.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.040818063614607
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:	PI-0387991.exe

General

File size:	899584
MD5:	655318bec9b30d5a2f2dedf399d87438
SHA1:	23f37c9bddcd8393f499fee9b77220765288020c
SHA256:	8cd1a5c6360cc1c0e513d4cc39f649bcb33b61c47c4b498b992ea8e9a41a48cd
SHA512:	1d9c8a2c6b29a73aca4ec5df29fd3300e9952ce51dfee405e7b2968a0ca50c7c0c6453cf44c4c32fcefac44145accd66f442572ca9cb01fc2ebd468dfc6a42b4
SSDEEP:	12288:Ugl23M132q8bSfGiWum/YBiXqDXRXITzftEFe67O+NAwcFSMPQipP5q:Jl23Mz51BrMUh4/ftEFe+ipQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..... .....@.. ....@.....

File Icon

Icon Hash:	f0debeffdffeec70

Static PE Info

General

Entrypoint:	0x47f0ae
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:	0x60F8B1B2 [Wed Jul 21 23:45:54 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	0x7d0b4	0x7d200	False	0.852360530095	data	7.71928782893	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x5e320	0x5e400	False	0.167336704244	data	5.64062676642	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	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
07/22/21-15:06:46.822458	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49695	34.102.136.180	192.168.2.5
07/22/21-15:06:52.270948	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49696	80	192.168.2.5	162.241.2.50
07/22/21-15:06:52.270948	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49696	80	192.168.2.5	162.241.2.50
07/22/21-15:06:52.270948	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49696	80	192.168.2.5	162.241.2.50
07/22/21-15:06:58.046372	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49697	34.102.136.180	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 15:06:35.140733957 CEST	192.168.2.5	8.8.8.8	0x9d59	Standard query (0)	www.romahony.com	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:41.487222910 CEST	192.168.2.5	8.8.8.8	0xf92a	Standard query (0)	www.bodymoisturizer.online	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:46.566061020 CEST	192.168.2.5	8.8.8.8	0xd1e8	Standard query (0)	www.idookap.com	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:51.908016920 CEST	192.168.2.5	8.8.8.8	0xdc94	Standard query (0)	www.siteoficial-liquida.com	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:57.778142929 CEST	192.168.2.5	8.8.8.8	0x7ce	Standard query (0)	www.hispanicassoclv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 15:06:35.602511883 CEST	8.8.8.8	192.168.2.5	0x9d59	No error (0)	www.romahony.com		103.120.82.56	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:41.550591946 CEST	8.8.8.8	192.168.2.5	0xf92a	Name error (3)	www.bodymoisturizer.online	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:46.629306078 CEST	8.8.8.8	192.168.2.5	0xd1e8	No error (0)	www.idookap.com	idookap.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 15:06:46.629306078 CEST	8.8.8.8	192.168.2.5	0xd1e8	No error (0)	idookap.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:52.109452009 CEST	8.8.8.8	192.168.2.5	0xdc94	No error (0)	www.siteoficial-liquida.com	siteoficial-liquida.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 15:06:52.109452009 CEST	8.8.8.8	192.168.2.5	0xdc94	No error (0)	siteoficial-liquida.com		162.241.2.50	A (IP address)	IN (0x0001)
Jul 22, 2021 15:06:57.859669924 CEST	8.8.8.8	192.168.2.5	0x7ce	No error (0)	www.hispanicassoclv.com	hispanicassoclv.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 15:06:57.859669924 CEST	8.8.8.8	192.168.2.5	0x7ce	No error (0)	hispanicassoclv.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.romahony.com
- www.idookap.com
- www.siteoficial-liquida.com
- www.hispanicassoclv.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49694	103.120.82.56	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 15:06:35.950139046 CEST	306	OUT	GET /q4kr/?m4z=hZWT6D&KdPxHVdh=stDcKtJiFThdGrRpndYyQbsbrCSX1QkCWnDTnTci+riMDIV/FP53rWURHHZjowo3ayyv HTTP/1.1 Host: www.romahony.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 15:06:51.325894117 CEST	308	IN	HTTP/1.1 404 Not Found Date: Thu, 22 Jul 2021 13:06:49 GMT Server: Apache/2.4.41 (Ubuntu) Status: 404 Not Found Vary: Accept-Encoding referer: http://image.baidu.com Content-Length: 0 Connection: close Content-Type: text/html;charset=utf-8;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49695	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 15:06:46.675175905 CEST	307	OUT	GET /q4kr/?m4z=hZWT6D&KdPxHVdh=8Twh4s36gZRno0YiIaK1Aog0Jq5SRxj1tGC/kNtcN6cj6UbdIOqmSeR7M7wA7kAlsS0+ HTTP/1.1 Host: www.idookap.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 15:06:46.822458029 CEST	307	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 22 Jul 2021 13:06:46 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef677e-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49696	162.241.2.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 15:06:52.270947933 CEST	308	OUT	GET /q4kr/?KdPxHVdh=UTB9cmVppYOj/UC3W28IAi1vRKY7uisBtiUczDixbM3KLxocs5bu1DNZcq72D06e9ENr&m4z=hZWT6D HTTP/1.1 Host: www.siteoficial-liquida.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 15:06:52.987106085 CEST	309	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 22 Jul 2021 13:06:52 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://siteoficial-liquida.com/q4kr/?KdPxHVdh=UTB9cmVppYOj/UC3W28IAi1vRKY7uisBtiUczDixbM3KLxocs5bu1DNZcq72D06e9ENr&m4z=hZWT6D Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49697	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 15:06:57.906836987 CEST	310	OUT	GET /q4kr/?m4z=hZWT6D&KdPxHVdh=+adpk/1z85ABQgFM8KoV7nh2RN9wNRyN3NacL4PKZthW2WB1UYKLVSKaUBe2HmlTnYf8 HTTP/1.1 Host: www.hispanicassoclv.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 15:06:58.046371937 CEST	311	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 22 Jul 2021 13:06:57 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef677e-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PI-0387991.exe PID: 5736 Parent PID: 5600

General

Start time:	15:04:49
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\PI-0387991.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI-0387991.exe'
Imagebase:	0xf90000
File size:	899584 bytes
MD5 hash:	655318BEC9B30D5A2F2DEDF399D87438
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.322811703.0000000004381000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.322811703.0000000004381000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.322811703.0000000004381000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.321727196.0000000003381000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 3328 Parent PID: 5736

General

Start time:	15:05:32
Start date:	22/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7ff797770000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000008.00000002.377469940.0000000000E30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.377469940.0000000000E30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.377469940.0000000000E30000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.377521591.0000000000E60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.377521591.0000000000E60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.377521591.0000000000E60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.377252491.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.377252491.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.377252491.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 3328

General

Start time:	15:05:34
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 5076 Parent PID: 3472

General

Start time:	15:05:55
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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.00000002.497338116.0000000003390000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.497338116.0000000003390000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.497338116.0000000003390000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.498996789.00000000039D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.498996789.00000000039D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.498996789.00000000039D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.499283578.0000000003A00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.499283578.0000000003A00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.499283578.0000000003A00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4860 Parent PID: 5076

General

Start time:	15:06:00
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1064 Parent PID: 4860

General

Start time:	15:06:00
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis