ID: 830617
Sample Name: PO_7413.exe
Cookbook: default.jbs
Time: 14:46:21
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

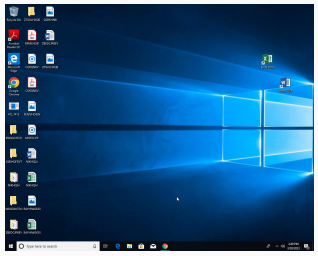
Windows Analysis Report

PO_7413.exe

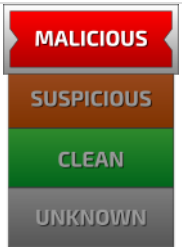
Overview

General Information

Sample Name:	PO_7413.exe
Analysis ID:	830617
MD5:	1b3b644b4869…
SHA1:	2a26e739cae6…
SHA256:	79bcc176d961…
Tags:	agenttesla exe
Infos:	



Detection



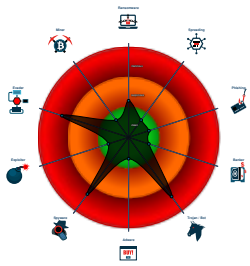
AgentTesla, zgRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- Malicious sample detected (through…
- Yara detected AgentTesla
- 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…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- PO_7413.exe (PID: 3084 cmdline: C:\Users\user\Desktop\PO_7413.exe MD5: 1B3B644B48693FFEA0D42032E778906B)
  - PO_7413.exe (PID: 6100 cmdline: C:\Users\user\Desktop\PO_7413.exe MD5: 1B3B644B48693FFEA0D42032E778906B)
  - PO_7413.exe (PID: 4636 cmdline: C:\Users\user\Desktop\PO_7413.exe MD5: 1B3B644B48693FFEA0D42032E778906B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Name	Description	Attribution	Blogpost URLs	Link
zgRAT		No Attribution	http://https://bazaar.abuse.ch/browse/signature/zgRAT/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.zgrat

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.printshopgt.com",
  "Username": "recepcion@printshopgt.com",
  "Password": "R3cGT17*"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.573339941.0000000002981000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.573339941.0000000002981000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: PO_7413.exe PID: 4636	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: PO_7413.exe PID: 4636	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO_7413.exe.378e940.4.raw.unpack	JoeSecurity_zgRAT_1	Yara detected zgRAT	Joe Security	
0.2.PO_7413.exe.378e940.4.raw.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x70b4b:$s1: file:/// • 0x70a5b:$s2: {11111-22222-10009-11112} • 0x70adb:$s3: {11111-22222-50001-00000} • 0x700dd:$s4: get_Module • 0x70368:$s5: Reverse • 0x14b5c0:$s5: Reverse • 0x6e1f4:$s6: BlockCopy • 0x14cc43:$s6: BlockCopy • 0x14b766:$s7: ReadByte • 0x70b5d:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.5 - Destination IP: 66.96.134.29

Timestamp:	192.168.2.566.96.134.29496905872839723 03/20/23-14:47:40.789390
SID:	2839723
Source Port:	49690
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.5 - Destination IP: 66.96.134.29

Timestamp:	192.168.2.566.96.134.29496905872851779 03/20/23-14:47:40.789531
SID:	2851779
Source Port:	49690
Destination Port:	587
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.5 - Destination IP: 66.96.134.29	
Timestamp:	192.168.2.566.96.134.29496905872840032 03/20/23-14:47:40.789531
SID:	2840032
Source Port:	49690
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.5 - Destination IP: 66.96.134.29	
Timestamp:	192.168.2.566.96.134.29496905872030171 03/20/23-14:47:40.789390
SID:	2030171
Source Port:	49690
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected zgRAT

Yara detected AgentTesla

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 browser information (history, passwords, etc)

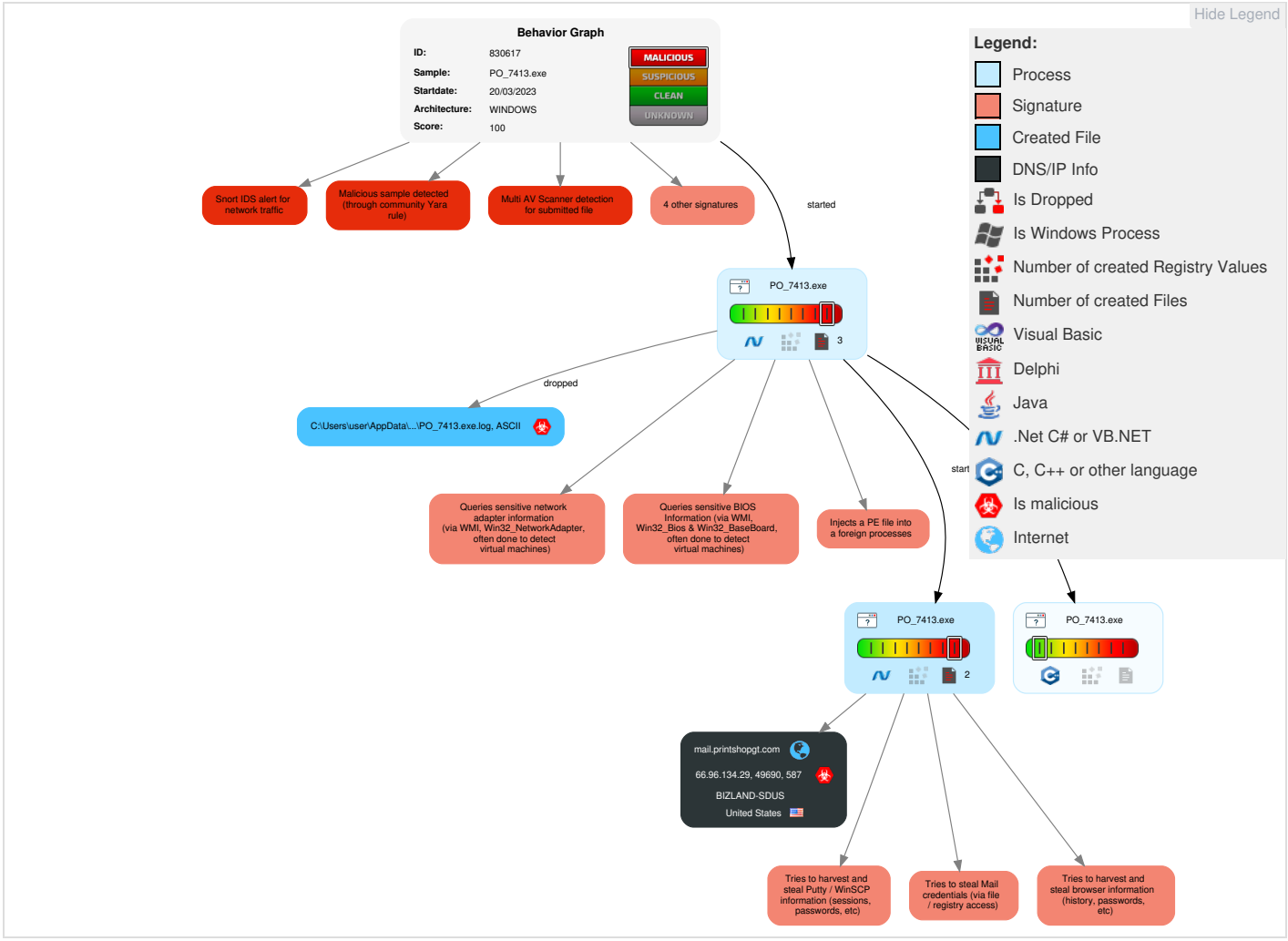
Remote Access Functionality

Yara detected zgRAT

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	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	1 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 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	1 Non-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 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 Account 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	3 Software Packing	Cached Domain Credentials	1 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	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 1 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

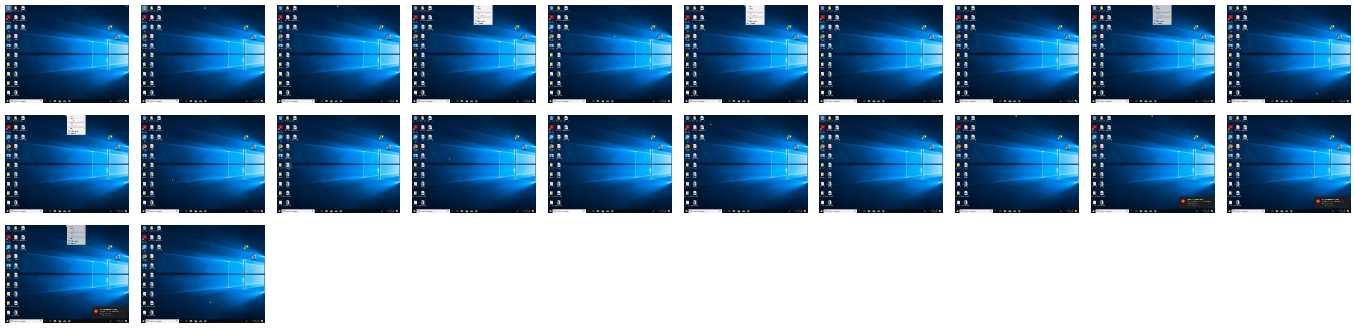
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO_7413.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
PO_7413.exe	40%	Virustotal		Browse
PO_7413.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.PO_7413.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/roso	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://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cns	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.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/T	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.com7	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.compef	0%	URL Reputation	safe	
http://www.fontbureau.comeded	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/K	0%	URL Reputation	safe	
http://www.carterandcone.comr	0%	URL Reputation	safe	
http://www.fontbureau.commK	0%	URL Reputation	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.carterandcone.coms	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd%	0%	Avira URL Cloud	safe	
http://www.sakkal.coms	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/x	0%	Avira URL Cloud	safe	
http://www.carterandcone.comms	0%	Avira URL Cloud	safe	
http://en.wu	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/g	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/on	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
http://www.fontbureau.comd	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.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.fontbureau.comdTTF	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comsiva7	0%	Avira URL Cloud	safe	
http://www.carterandcone.comand	0%	URL Reputation	safe	
http://mail.printshopgt.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cntyp	0%	Avira URL Cloud	safe	
http://www.carterandcone.comJl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.printshopgt.com	66.96.134.29	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comen	PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd%	PO_7413.exe, 00000000.00000003.313872425.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313999190.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	PO_7413.exe, 00000000.00000003.310758013.000000000575F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313041787.0000000005722000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312856168.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsF	PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314250685.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/roso	PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO_7413.exe, 00000000.00000002.350675185.000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/7	PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312706788.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312621841.0000000005736000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.coms	PO_7413.exe, 00000000.00000003.313407677.0000000005728000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comB.TTF	PO_7413.exe, 00000000.00000003.313999190.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cns	PO_7413.exe, 00000000.00000003.309955974.0000000005723000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.309839200.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/x	PO_7413.exe, 00000000.00000003.314864766.000000000573A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/.	PO_7413.exe, 00000000.00000003.313331989.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312706788.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PO_7413.exe, 00000000.00000002.350675185.000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	PO_7413.exe, 00000000.00000003.313331989.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comms	PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.wu	PO_7413.exe, 00000000.00000003.306402390.0000000005743000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.306465269.0000000005743000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.306497370.0000000005742000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.306380254.0000000005742000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.306358175.0000000005743000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	PO_7413.exe, 00000000.00000003.309091289.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.307673660.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.307412713.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308652862.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308603977.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308204869.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308127982.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308409074.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.307090748.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.307291691.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308973363.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308162888.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.309149145.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.307957109.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308292309.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308917042.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308460070.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.307145904.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.308862175.000000000575F000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.307814144.000000000575F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.309358449.0000000000B1C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/T	PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com7	PO_7413.exe, 00000000.00000003.313872425.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313999190.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	PO_7413.exe, 00000000.00000003.314488615.000000000572C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

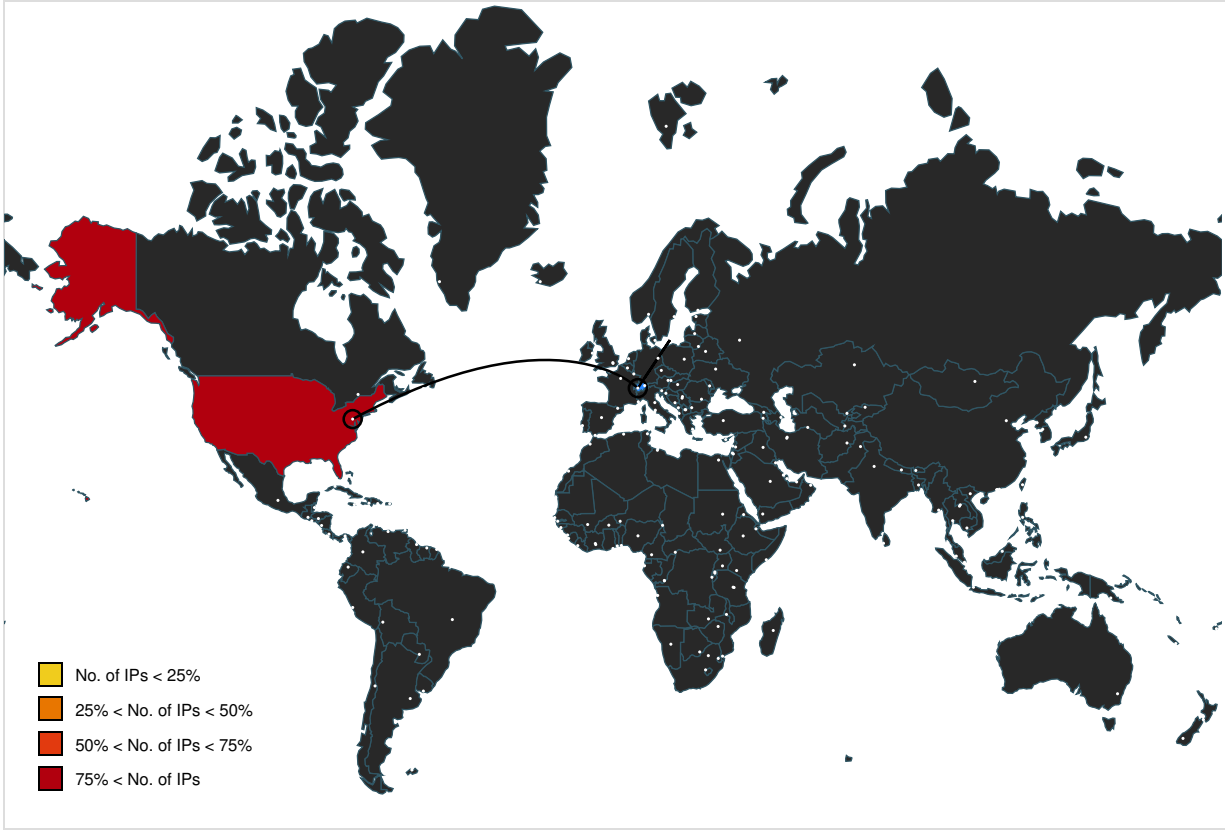
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.come	PO_7413.exe, 00000000.00000003.306497370.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/g	PO_7413.exe, 00000000.00000003.314864766.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.compef	PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PO_7413.exe, 00000000.00000003.313872425.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314590924.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313999190.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314060524.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comeded	PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313999190.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314250685.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314060524.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314133005.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/	PO_7413.exe, 00000000.00000003.314864766.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314864766.000000000573A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314250685.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314133005.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/T	PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312706788.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/K	PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312706788.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comr	PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commK	PO_7413.exe, 00000000.00000003.321613204.0000000005720000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlic	PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314250685.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314133005.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coms	PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/on	PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312706788.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.wikip	PO_7413.exe, 00000000.00000003.309795226.0000000005743000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.309639619.0000000005740000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.309866819.0000000005743000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314250685.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comsiva7	PO_7413.exe, 00000000.00000003.314133005.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	PO_7413.exe, 00000000.00000003.310287732.0000000005743000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.310370311.0000000005740000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.310481524.0000000005743000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.printshopgt.com	PO_7413.exe, 00000002.00000002.573339941.00000000029D9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	PO_7413.exe, 00000000.00000002.350675185.0000000006932000.00000004.00000800.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.310155887.000000000572D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	PO_7413.exe, 00000000.00000003.313331989.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313437350.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/s	PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdTTF	PO_7413.exe, 00000000.00000003.313872425.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.	PO_7413.exe, 00000000.00000003.314712938.000000000572A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/o	PO_7413.exe, 00000000.00000003.313331989.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312706788.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312621841.0000000005736000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlvfet	PO_7413.exe, 00000000.00000003.321613204.0000000005720000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comm	PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314250685.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314133005.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	PO_7413.exe, 00000000.00000003.312621841.0000000005736000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO_7413.exe, 00000000.00000002.350675185.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	PO_7413.exe, 00000000.00000003.314396930.0000000005735000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314488615.0000000005739000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.314315988.0000000005735000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/e	PO_7413.exe, 00000000.00000003.313176984.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312826759.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312890011.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312706788.000000000573B000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312994530.000000000573B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comJl	PO_7413.exe, 00000000.00000003.312919072.0000000005722000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.313041787.0000000005722000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.312856168.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comand	PO_7413.exe, 00000000.00000003.312009586.0000000005722000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cntyp	PO_7413.exe, 00000000.00000003.309795226.0000000005743000.00000004.00000020.00020000.00000000.sdmp, PO_7413.exe, 00000000.00000003.309866819.0000000005743000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.96.134.29	mail.printshopgt.com	United States		29873	BIZLAND-SDUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830617
Start date and time:	2023-03-20 14:46:21 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	6
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
Sample file name:	PO_7413.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@1/1
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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
14:47:25	API Interceptor	19x Sleep call for process: PO_7413.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\PO_7413.exe.log

Process:	C:\Users\user\Desktop\PO_7413.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C

SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8746286820631415
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:	PO_7413.exe
File size:	921600
MD5:	1b3b644b48693ffea0d42032e778906b
SHA1:	2a26e739cae611522e94853194499765aa7ba30c
SHA256:	79bcc176d961b06ff3f7af0000c16e8fae56cf03b504153e439ecbccfaa34bbf
SHA512:	5889b4312b50de48da9e57d0eeba34ffe7f552f9213168e968987150752c353ddf9191b421ef89ec32249002d261f252eb34870320d1cc61b630e8f0102ccad7
SSDEEP:	24576:FKUX6CbNDSMEBscggDeSOrwBNKDAsJvZ:pXZbIXBxeS5BNKr7
TLSH:	4A1502246BEB8326F6365BBD91A12682577E27A37703D68D1CF112CA4727B014FD132B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..._.....0.....%... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e25aa
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:	0xE7AB8A5F [Sun Mar 1 20:49:35 2093 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
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
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	0xe2558	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe4000	0x58c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xe035c	0x70	.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	0xe05b0	0xe0600	False	0.936121387534819	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.880495014103316	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0x58c	0x600	False	0.4173177083333333	data	4.044715606987517	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe6000	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	0xe4090	0x2fc	data		
RT_MANIFEST	0xe439c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

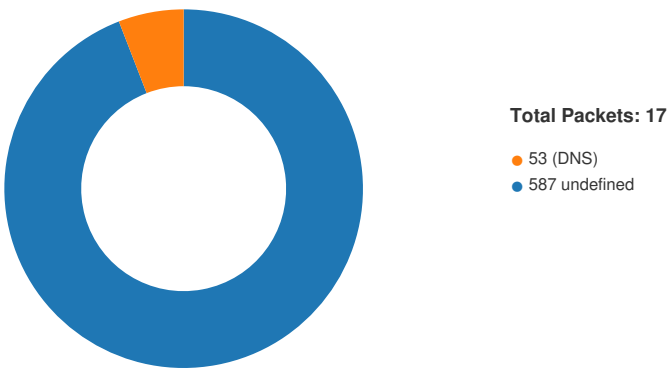
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.566.96.134.29496905872839723 03/20/23-14:47:40.789390	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49690	587	192.168.2.5	66.96.134.29
192.168.2.566.96.134.29496905872851779 03/20/23-14:47:40.789531	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49690	587	192.168.2.5	66.96.134.29
192.168.2.566.96.134.29496905872840032 03/20/23-14:47:40.789531	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49690	587	192.168.2.5	66.96.134.29
192.168.2.566.96.134.29496905872030171 03/20/23-14:47:40.789390	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49690	587	192.168.2.5	66.96.134.29

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 14:47:38.902317047 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:39.007510900 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.007812023 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:39.114033937 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.119223118 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:39.224498987 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.224586964 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.225270033 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:39.330396891 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.330877066 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.331320047 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:39.436825037 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.438386917 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.438667059 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:39.544048071 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.546717882 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:39.546988964 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:39.652383089 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:40.681462049 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:40.681699991 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:40.787223101 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:40.787426949 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:40.789390087 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:40.789530993 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:40.789588928 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:40.789647102 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:47:40.894815922 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:40.894861937 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:40.896704912 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:47:41.036768913 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:49:19.270958900 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:49:19.376615047 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:49:19.377424002 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:49:19.377515078 CET	587	49690	66.96.134.29	192.168.2.5
Mar 20, 2023 14:49:19.377933025 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:49:19.380515099 CET	49690	587	192.168.2.5	66.96.134.29
Mar 20, 2023 14:49:19.485925913 CET	587	49690	66.96.134.29	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 14:47:38.769144058 CET	58218	53	192.168.2.5	8.8.8.8
Mar 20, 2023 14:47:38.882294893 CET	53	58218	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 14:47:38.769144058 CET	192.168.2.5	8.8.8.8	0x699a	Standard query (0)	mail.print shopgt.com	A (IP address)	IN (0x0001)	false

DNS Answers

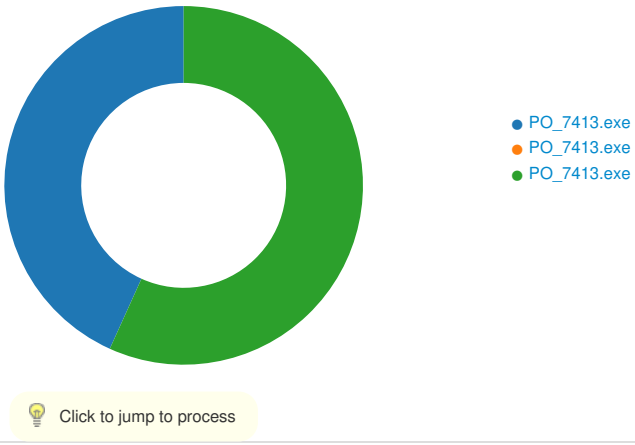
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 14:47:38.882294893 CET	8.8.8.8	192.168.2.5	0x699a	No error (0)	mail.print shopgt.com		66.96.134.29	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 20, 2023 14:47:39.114033937 CET	587	49690	66.96.134.29	192.168.2.5	220 ESMTP Mon, 20 Mar 2023 09:47:39 -0400: UCE strictly prohibited
Mar 20, 2023 14:47:39.119223118 CET	49690	587	192.168.2.5	66.96.134.29	EHLO 367706
Mar 20, 2023 14:47:39.224586964 CET	587	49690	66.96.134.29	192.168.2.5	250-bosauthsmtp04.yourhostingaccount.com Hello 367706 [84.17.52.9] 250-SIZE 34603008 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250 HELP
Mar 20, 2023 14:47:39.225270033 CET	49690	587	192.168.2.5	66.96.134.29	AUTH login cmVjZXBjaW9uQHByaW50c2hvcGd0LmNvbQ==
Mar 20, 2023 14:47:39.330877066 CET	587	49690	66.96.134.29	192.168.2.5	334 UGFzc3dvcmQ6
Mar 20, 2023 14:47:39.438386917 CET	587	49690	66.96.134.29	192.168.2.5	235 Authentication succeeded
Mar 20, 2023 14:47:39.438667059 CET	49690	587	192.168.2.5	66.96.134.29	MAIL FROM:<recepcion@printshopgt.com>
Mar 20, 2023 14:47:39.546717882 CET	587	49690	66.96.134.29	192.168.2.5	250 OK
Mar 20, 2023 14:47:39.546988964 CET	49690	587	192.168.2.5	66.96.134.29	RCPT TO:<recepcion@printshopgt.com>
Mar 20, 2023 14:47:40.681462049 CET	587	49690	66.96.134.29	192.168.2.5	250 Accepted
Mar 20, 2023 14:47:40.681699991 CET	49690	587	192.168.2.5	66.96.134.29	DATA
Mar 20, 2023 14:47:40.787426949 CET	587	49690	66.96.134.29	192.168.2.5	354 Enter message, ending with "." on a line by itself
Mar 20, 2023 14:47:40.789647102 CET	49690	587	192.168.2.5	66.96.134.29	.
Mar 20, 2023 14:47:40.896704912 CET	587	49690	66.96.134.29	192.168.2.5	250 OK id=1peFrQ-00054x-Nh
Mar 20, 2023 14:49:19.270958900 CET	49690	587	192.168.2.5	66.96.134.29	QUIT
Mar 20, 2023 14:49:19.377424002 CET	587	49690	66.96.134.29	192.168.2.5	221 bosauthsmtp04.yourhostingaccount.com closing connection

Statistics

Behavior



System Behavior

Analysis Process: PO_7413.exe PID: **3084**, Parent PID: **3324**

General

Target ID:	0
Start time:	14:47:19
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\PO_7413.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO_7413.exe

Imagebase:	0x10000
File size:	921600 bytes
MD5 hash:	1B3B644B48693FFEA0D42032E778906B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	7226CF06	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	7226CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_7413.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7257C78D	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\PO_7413.exe.log	0	1216	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	7257C907	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	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72245705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7224CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721A03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	710B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	710B1B4F	ReadFile

Analysis Process: PO_7413.exe PID: **6100**, Parent PID: **3084**

General

Target ID:	1
Start time:	14:47:27
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\PO_7413.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO_7413.exe
Imagebase:	0x80000
File size:	921600 bytes
MD5 hash:	1B3B644B48693FFEA0D42032E778906B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO_7413.exe PID: **4636**, Parent PID: **3084**

General

Target ID:	2
Start time:	14:47:27
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\PO_7413.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO_7413.exe
Imagebase:	0x4d0000
File size:	921600 bytes
MD5 hash:	1B3B644B48693FFEA0D42032E778906B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.573339941.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.573339941.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	7226CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7226CF06	unknown

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	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72245705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7224CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	710B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	710B1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	710B1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	710B1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	710B1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	710B1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	710B1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	710B1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	710B1B4F	ReadFile

Disassembly

No disassembly