ID: 356838
Sample Name: ST_PLC URGENT ORDER 0223308737,pdf.exe
Cookbook: default.jbs
Time: 17:36:45
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report ST_PLC URGENT ORDER 0223308737,pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Snake Keylogger 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Networking: 5
System Summary: 6
Data Obfuscation: 6
Malware Analysis System Evasion: 6
Anti Debugging: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 13
Public 13
General Information 13
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 16
ASN 17
JA3 Fingerprints 17
Dropped Files 18
Created / dropped Files 18
Static File Info 18
General 18
File Icon 19
Static PE Info 19
General 19

Entrypoint Preview 19
Data Directories 21
Sections 21
Resources 21
Imports 21
Version Infos 22
Network Behavior 22
Network Port Distribution 22
TCP Packets 22
UDP Packets 23
DNS Queries 24
DNS Answers 24
HTTP Request Dependency Graph 25
HTTP Packets 25
HTTPS Packets 26
Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: ST_PLC URGENT ORDER 0223308737,pdf.exe PID: 6256 Parent PID: 5708 27
General 27
File Activities 27
File Created 27
File Written 27
File Read 28
Analysis Process: ST_PLC URGENT ORDER 0223308737,pdf.exe PID: 5656 Parent PID: 6256 28
General 28
File Activities 29
File Created 29
File Deleted 29
File Read 29
Registry Activities 29
Disassembly 30
Code Analysis 30

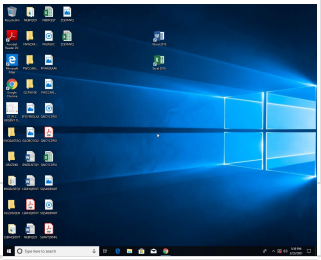
Analysis Report ST_PLC URGENT ORDER 0223308737,...

Overview

General Information

Sample Name:	ST_PLC URGENT ORDER 0223308737,pdf.exe
Analysis ID:	356838
MD5:	49b05de1926be1..
SHA1:	92caf8d81c1cdda..
SHA256:	f5a3420b7aa30f9..
Tags:	exe SnakeKeylogger
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

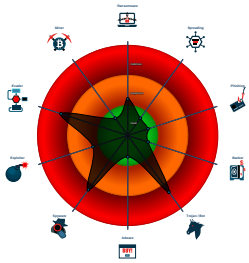
Snake Keylogger

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected Snake Keylogger
- Contains functionality to check if a d...
- Initial sample is a PE file and has a ...
- Injects a PE file into a foreign proce...
- Machine Learning detection for samp...
- May check the online IP address of ...
- PE file contains section with special...
- PE file has nameless sections
- Tries to harvest and steal browser in...
- Tries to steal Mail credentials (via fil...

Classification



Startup

- **System is w10x64**
- ST_PLC URGENT ORDER 0223308737,pdf.exe (PID: 6256 cmdline: 'C:\Users\user\Desktop\ST_PLC URGENT ORDER 0223308737,pdf.exe' MD5: 49B05DE1926BE1EA5993874AD14C8D3A)
  - ST_PLC URGENT ORDER 0223308737,pdf.exe (PID: 5656 cmdline: {path} MD5: 49B05DE1926BE1EA5993874AD14C8D3A)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": {
    "Port": "587",
    "SMTP Credential": "info@endovision.xyzr)($czxJs0smtp.endovision.xyz"
  }
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.502527744.000000000402000.00000040.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000009.00000002.502527744.000000000402000.00000040.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000000.00000002.326366120.000000000361000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000000.00000002.326366120.000000000361000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: ST_PLC URGENT ORDER 0223308737,pdf.exe PID: 6256	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 4 entries				

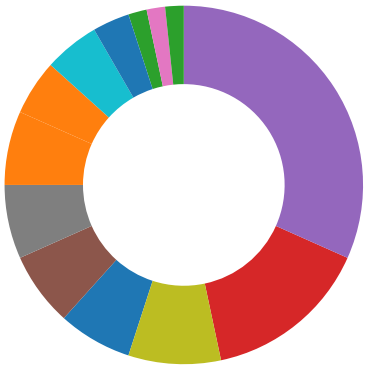
Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.ST_PLC URGENT ORDER 0223308737,pdf.exe.400000.0.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
9.2.ST_PLC URGENT ORDER 0223308737,pdf.exe.400000.0.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.ST_PLC URGENT ORDER 0223308737,pdf.exe.36fb770.3.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.ST_PLC URGENT ORDER 0223308737,pdf.exe.36fb770.3.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.ST_PLC URGENT ORDER 0223308737,pdf.exe.36fb770.3.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses insecure TLS / SSL version for HTTPS connection

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

May check the online IP address of the machine

System Summary:

Initial sample is a PE file and has a suspicious name

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Yara detected Beds Obfuscator

Malware Analysis System Evasion:

Yara detected Beds Obfuscator

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Snake Keylogger

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

Tries to steal Mail credentials (via file access)

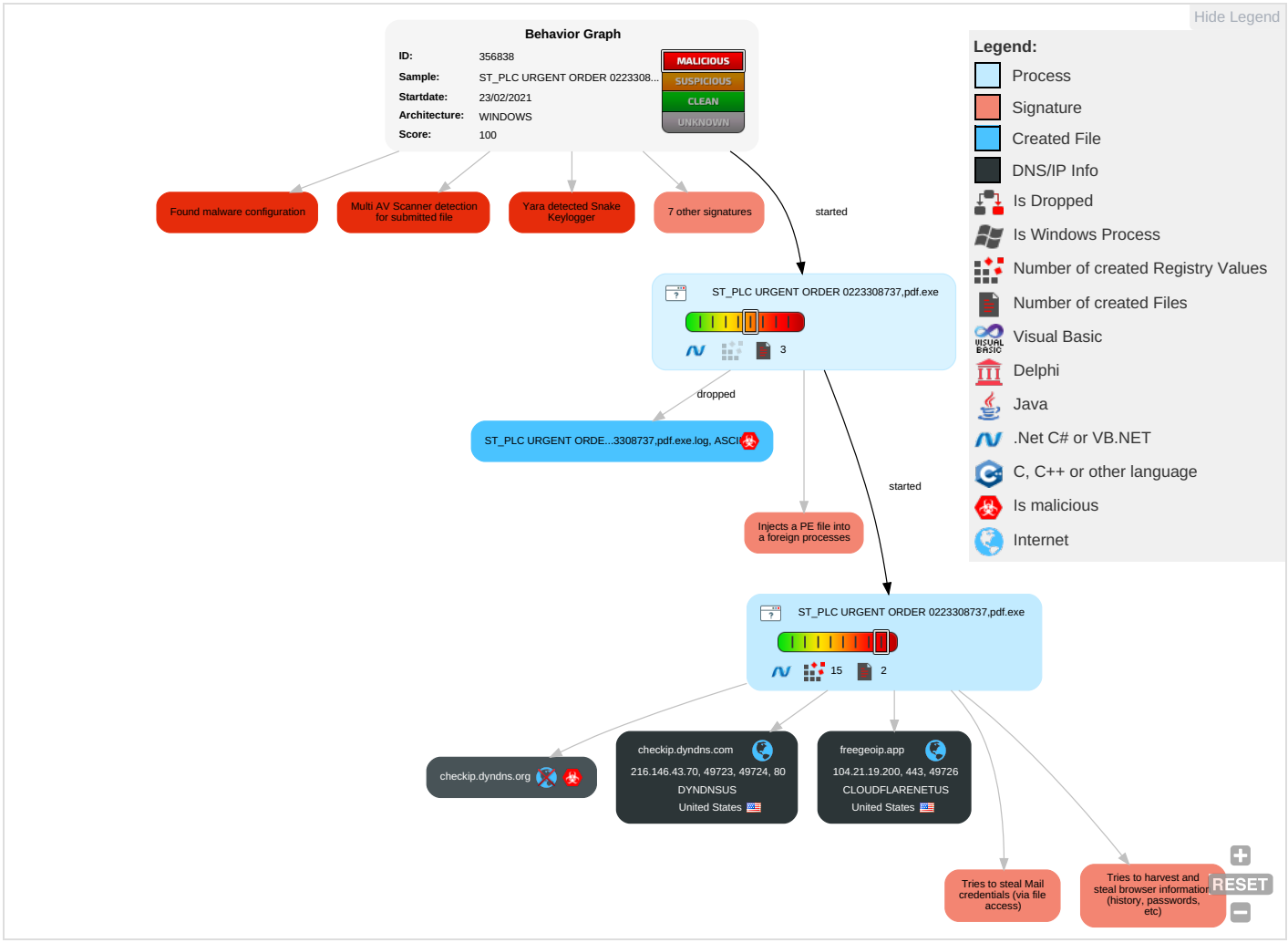
Remote Access Functionality:

Yara detected Snake Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 4	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service

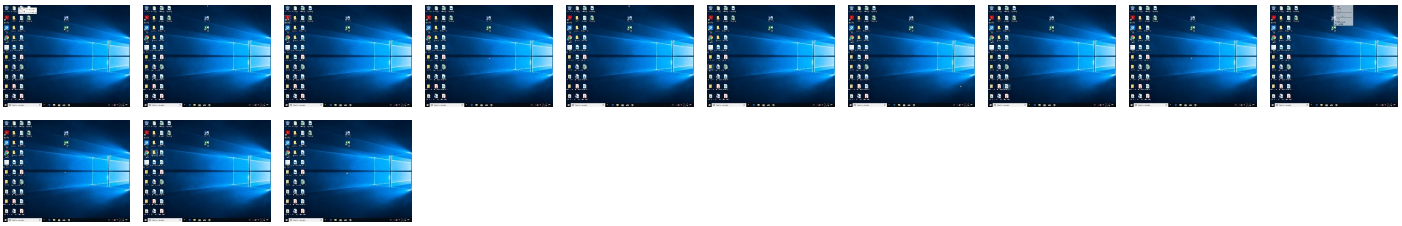
Behavior Graph



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
ST_PLC URGENT ORDER 0223308737,pdf.exe	32%	ReversingLabs	Win32.Trojan.AgentTesla	
ST_PLC URGENT ORDER 0223308737,pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.ST_PLC URGENT ORDER 0223308737,pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
0.2.ST_PLC URGENT ORDER 0223308737,pdf.exe.190000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

Source	Detection	Scanner	Label	Link
freegeoip.app	0%	Virustotal		Browse
checkip.dyndns.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comits)	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.founder.com.cn/cnv-s	0%	Avira URL Cloud	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://checkip.dyndns.org/HB:l0A	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://en.wU	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://www.agfamonotype.t	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn-u	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnold	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comue	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnva	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8ok	0%	Avira URL Cloud	safe	
http://https://freegeoip.app4okl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
freegeoip.app	104.21.19.200	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.com	216.146.43.70	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://www.carterandcone.comits)	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 1379781.0000000007CAA000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/?	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comva	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 1183518.0000000007CDE000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnv-s	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 0657129.0000000007CDE000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9508033.0000000003206000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org/HB:l0A	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9245572.00000000031B1000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wU	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 0592808.0000000007CA5000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://www.goodfont.co.kr	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnC	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 0451930.0000000007CDE000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.agfamonotype.t	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.32 3215970.0000000007CA0000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrito	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.32 4374669.0000000000BD7000.00000 004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot/sendMessage?chat_id=&text=Createutf-8	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9245572.00000000031B1000.00000 004.00000001.sdmp	false		high
http://www.founder.com.cn/cnn-u	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 0625033.0000000007CBB000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.com	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9435893.00000000031FD000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9245572.00000000031B1000.00000 004.00000001.sdmp	false		high
http://www.sakkal.com	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://freegeoip.app	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9508033.0000000003206000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://freegeoip.app/xml/	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9508033.0000000003206000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://www.fontbureau.com	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://www.founder.com.cn/cnold	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 0625033.0000000007CBB000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comue	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.32 4374669.0000000000BD7000.00000 004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9245572.00000000031B1000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/84.17.52.38x	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9508033.0000000003206000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://freegeoip.app/xml/LoadCountryNameClipboard	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9245572.00000000031B1000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 0789901.0000000007CDE000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 0625033.0000000007CBB000.00000 004.00000001.sdmp, ST_PLC URGENT ORDER 0223308737,pdf.exe, 0 0000000.00000003.240840157.000 0000007CDE000.00000004.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://www.zhongyicts.com.cnva	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000003.24 1159879.0000000007CDF000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000000.00000002.33 3635479.0000000007D90000.00000 002.00000001.sdmp	false		high
http://https://freegeoip.app/xml/84.17.52.38	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9508033.0000000003206000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.orgD8ok	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9508033.0000000003206000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app4okl	ST_PLC URGENT ORDER 0223308737 ,pdf.exe, 00000009.00000002.50 9508033.0000000003206000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.146.43.70	unknown	United States		33517	DYNDNSUS	false
104.21.19.200	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356838
Start date:	23.02.2021
Start time:	17:36:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ST_PLC URGENT ORDER 0223308737,pdf.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@3/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.42.151.234, 51.11.168.160, 40.88.32.150, 13.88.21.125, 104.43.139.144, 23.211.6.115, 23.218.208.56, 52.147.198.201, 2.20.142.210, 2.20.142.209, 8.253.207.120, 8.248.97.254, 8.238.85.126, 8.241.80.126, 8.248.115.254, 51.103.5.186, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
17:37:44	API Interceptor	1x Sleep call for process: ST_PLC URGENT ORDER 0223308737,pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
216.146.43.70	QUOTE.doc	Get hash	malicious	Browse	• checkip.dyndns.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9073782912,pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SwiftCopyTT.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SHIPPING DOCUMENTS_PDF.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Product Specification#742852.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PO-SCHF-CCM_NFI_FSL-RED-20-01 001-A.PDF.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	DHL_Receipt Document_7368638172,pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	pay09809988.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Medisave Order 180827.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	New_Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PO on demand 4000270283-B60.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PO.xls	Get hash	malicious	Browse	• checkip.dyndns.org/
	Quotes.xlsm	Get hash	malicious	Browse	• checkip.dyndns.org/
	Purchase Orde.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	DHL_FORM_16022021.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
checkip.dyndns.com	P00760000.exe	Get hash	malicious	Browse	• 162.88.193.70
	Order.doc	Get hash	malicious	Browse	• 131.186.113.70
	QUOTE.doc	Get hash	malicious	Browse	• 216.146.43.70
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 131.186.113.70
	Purchase Order.exe	Get hash	malicious	Browse	• 131.186.113.70
	dot crypted.exe	Get hash	malicious	Browse	• 131.186.113.70
	v2.exe	Get hash	malicious	Browse	• 131.186.113.70
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 216.146.43.71
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 162.88.193.70
	FOB offer_1164087223_l0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 162.88.193.70
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 131.186.113.70
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order 1.exe	Get hash	malicious	Browse	• 162.88.193.70
freegeoip.app	P00760000.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.doc	Get hash	malicious	Browse	• 104.21.19.200
	QUOTE.doc	Get hash	malicious	Browse	• 104.21.19.200
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	v2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order 1.exe	Get hash	malicious	Browse	• 172.67.188.154

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DYNDNSUS	P00760000.exe	Get hash	malicious	Browse	• 162.88.193.70
	Order.doc	Get hash	malicious	Browse	• 162.88.193.70
	QUOTE.doc	Get hash	malicious	Browse	• 216.146.43.70
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 131.186.113.70
	Purchase Order.exe	Get hash	malicious	Browse	• 131.186.113.70
	dot crypted.exe	Get hash	malicious	Browse	• 131.186.113.70
	v2.exe	Get hash	malicious	Browse	• 131.186.113.70
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 216.146.43.71
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 162.88.193.70
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 162.88.193.70
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 131.186.113.70
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order 1.exe	Get hash	malicious	Browse	• 162.88.193.70
CLOUDFLARENETUS	SecuriteInfo.com.Trojan.GenericKD.45695593.9197.exe	Get hash	malicious	Browse	• 172.67.199.58
	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	Get hash	malicious	Browse	• 104.23.98.190
	1vuet1S3tI.exe	Get hash	malicious	Browse	• 172.67.199.58
	P00760000.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.doc	Get hash	malicious	Browse	• 104.21.19.200
	QUOTE.doc	Get hash	malicious	Browse	• 104.21.19.200
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	2070121_SN-WS.exe	Get hash	malicious	Browse	• 104.21.71.230
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	payment_advice.doc	Get hash	malicious	Browse	• 172.67.172.17
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 172.67.172.17
	Purchase Order list.exe	Get hash	malicious	Browse	• 104.21.23.61
	RkoKlvuLh6.exe	Get hash	malicious	Browse	• 162.159.13 6.232
	i0fOtOV8v0.exe	Get hash	malicious	Browse	• 104.23.99.190
	P3knxzE7wN.exe	Get hash	malicious	Browse	• 162.159.12 8.233

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	Get hash	malicious	Browse	• 104.21.19.200
	P00760000.exe	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	v2.exe	Get hash	malicious	Browse	• 104.21.19.200
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 104.21.19.200
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 104.21.19.200
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 104.21.19.200
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order 1.exe	Get hash	malicious	Browse	• 104.21.19.200
	telex transfer.exe	Get hash	malicious	Browse	• 104.21.19.200
	GPP.exe	Get hash	malicious	Browse	• 104.21.19.200

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ST_PLC URGENT ORDER 0223308737,pdf.exe.log

Process:	C:\Users\user\Desktop\ST_PLC URGENT ORDER 0223308737,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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):	7.9094410868579645
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%

General

File name:	ST_PLC URGENT ORDER 0223308737,pdf.exe
File size:	451584
MD5:	49b05de1926be1ea5993874ad14c8d3a
SHA1:	92caf8d81c1cddab1e799d730b6f31b8820bdef5
SHA256:	f5a3420b7aa30f99c877d5a661625e37b79841f4bc99bd17a75d46eb86e4791d
SHA512:	03f249e4037b9ca54a278b2179bb41d13635c11e1c5ac9e553850963953eaae9e06e9d130424afd599792949f61191a6efa203d17f02c31add73695171247da
SSDEEP:	12288:205SiHsQ5WL82LHE4NnJRbDJ51n4OhNl2Eo6:2qHRWLjHNLX1VNk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....4`.....0..I...t.....`...`... ....@.. .....@.....

File Icon

Icon Hash:	00870c0808c44c00

Static PE Info

General

Entrypoint:	0x47600a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6034FDA3 [Tue Feb 23 13:05:39 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00476000h]
add 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
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16988	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x48c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x74000	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	0x76000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x16000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
qd?b#D	0x2000	0x126dc	0x12800	False	1.00040910051	data	7.99769775695	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x16000	0x56920	0x56a00	False	0.935518691378	data	7.94788728273	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x48c8	0x4a00	False	0.250369510135	data	3.76229374867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x76000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6e130	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0x72358	0x14	data		
RT_VERSION	0x7236c	0x36c	data		
RT_MANIFEST	0x726d8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

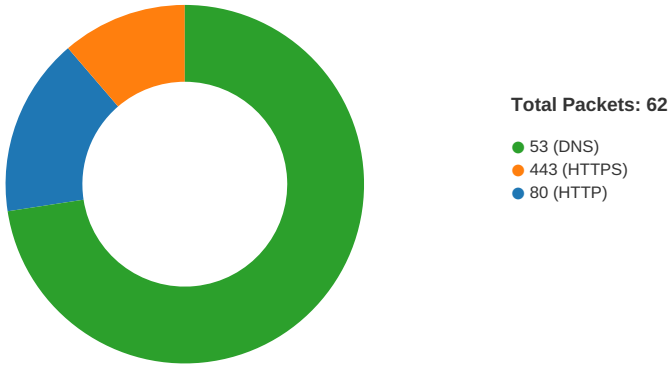
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Neudesic 2017
Assembly Version	1.0.0.0
InternalName	YGxk.exe
FileVersion	1.0.0.0
CompanyName	Neudesic
LegalTrademarks	
Comments	
ProductName	VectorBasedDrawing
ProductVersion	1.0.0.0
FileDescription	VectorBasedDrawing
OriginalFilename	YGxk.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:38:20.893306971 CET	49723	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:20.966469049 CET	80	49723	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:20.966756105 CET	49723	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:20.967432022 CET	49723	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:21.040594101 CET	80	49723	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.041201115 CET	80	49723	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.041230917 CET	80	49723	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.041450977 CET	49723	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:21.044296980 CET	49723	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:21.117485046 CET	80	49723	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.237832069 CET	49724	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:21.310719967 CET	80	49724	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.311430931 CET	49724	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:21.311459064 CET	49724	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:21.387285948 CET	80	49724	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.387928963 CET	80	49724	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.387953997 CET	80	49724	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:21.388036966 CET	49724	80	192.168.2.7	216.146.43.70
Feb 23, 2021 17:38:21.388557911 CET	49724	80	192.168.2.7	216.146.43.70

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:38:21.461718082 CET	80	49724	216.146.43.70	192.168.2.7
Feb 23, 2021 17:38:24.081542015 CET	49726	443	192.168.2.7	104.21.19.200
Feb 23, 2021 17:38:24.122629881 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.122745037 CET	49726	443	192.168.2.7	104.21.19.200
Feb 23, 2021 17:38:24.197956085 CET	49726	443	192.168.2.7	104.21.19.200
Feb 23, 2021 17:38:24.243032932 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.243081093 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.243105888 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.243175030 CET	49726	443	192.168.2.7	104.21.19.200
Feb 23, 2021 17:38:24.256527901 CET	49726	443	192.168.2.7	104.21.19.200
Feb 23, 2021 17:38:24.297560930 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.299608946 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.412383080 CET	49726	443	192.168.2.7	104.21.19.200
Feb 23, 2021 17:38:24.453402996 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.574615955 CET	443	49726	104.21.19.200	192.168.2.7
Feb 23, 2021 17:38:24.678195000 CET	49726	443	192.168.2.7	104.21.19.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:37:28.765932083 CET	58562	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:28.840821981 CET	53	58562	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:28.899852037 CET	56590	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:29.343880892 CET	60501	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:29.392760992 CET	53	60501	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:29.893305063 CET	56590	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:29.942009926 CET	53	56590	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:31.164011955 CET	53775	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:31.217535019 CET	53	53775	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:31.971314907 CET	51837	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:32.021707058 CET	53	51837	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:33.292634010 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:33.341347933 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:35.572705030 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:35.631392956 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:38.290208101 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:38.338884115 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:39.756915092 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:39.805471897 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:40.927508116 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:40.976974964 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:42.262983084 CET	58717	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:42.311651945 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:43.446369886 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:43.495011091 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:44.831759930 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:44.889130116 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:46.029300928 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:46.078305006 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:47.481002092 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:47.529805899 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:48.777369976 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:48.828838110 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:49.919188976 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:49.968007088 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:52.318013906 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:52.379735947 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:54.380870104 CET	52816	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:54.440943956 CET	53	52816	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:55.529963970 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:55.581351995 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:57.132116079 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:37:57.183653116 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 17:37:58.434371948 CET	54911	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:37:58.483202934 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:01.095828056 CET	49958	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:01.144601107 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:02.097351074 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:02.148971081 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:03.843122959 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:03.894375086 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:20.714721918 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:20.763413906 CET	53	59730	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:20.802294970 CET	59310	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:20.853791952 CET	53	59310	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:24.002441883 CET	51919	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:24.029129028 CET	64296	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:24.061353922 CET	53	51919	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:24.078514099 CET	53	64296	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:24.195754051 CET	56680	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:24.213799953 CET	58820	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:24.258230925 CET	53	56680	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:24.266051054 CET	53	58820	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:25.708842039 CET	60983	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:25.760257959 CET	53	60983	8.8.8.8	192.168.2.7
Feb 23, 2021 17:38:38.326183081 CET	49247	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:38:38.384884119 CET	53	49247	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:13.896173954 CET	52286	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:13.946187973 CET	53	52286	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:16.795876980 CET	56064	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:16.864464045 CET	53	56064	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:36.137834072 CET	63744	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:36.197748899 CET	53	63744	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:37.202028990 CET	61457	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:37.267780066 CET	53	61457	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:37.856884956 CET	58367	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:37.946634054 CET	53	58367	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:38.473057985 CET	60599	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:38.526653051 CET	59571	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:38.550015926 CET	53	60599	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:38.583594084 CET	53	59571	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:39.255326033 CET	52689	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:39.312680006 CET	53	52689	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:39.935694933 CET	50290	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:40.023211956 CET	53	50290	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:40.629940987 CET	60427	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:40.689760923 CET	53	60427	8.8.8.8	192.168.2.7
Feb 23, 2021 17:39:41.575957060 CET	56209	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:39:41.638529062 CET	53	56209	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:38:20.714721918 CET	192.168.2.7	8.8.8.8	0x9b1e	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.802294970 CET	192.168.2.7	8.8.8.8	0xfa3c	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:24.029129028 CET	192.168.2.7	8.8.8.8	0xef52	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:38:20.763413906 CET	8.8.8.8	192.168.2.7	0x9b1e	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:38:20.763413906 CET	8.8.8.8	192.168.2.7	0x9b1e	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:38:20.763413906 CET	8.8.8.8	192.168.2.7	0x9b1e	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.763413906 CET	8.8.8.8	192.168.2.7	0x9b1e	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.763413906 CET	8.8.8.8	192.168.2.7	0x9b1e	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.763413906 CET	8.8.8.8	192.168.2.7	0x9b1e	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.853791952 CET	8.8.8.8	192.168.2.7	0xfa3c	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:38:20.853791952 CET	8.8.8.8	192.168.2.7	0xfa3c	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.853791952 CET	8.8.8.8	192.168.2.7	0xfa3c	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.853791952 CET	8.8.8.8	192.168.2.7	0xfa3c	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.853791952 CET	8.8.8.8	192.168.2.7	0xfa3c	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:20.853791952 CET	8.8.8.8	192.168.2.7	0xfa3c	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:24.078514099 CET	8.8.8.8	192.168.2.7	0xef52	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Feb 23, 2021 17:38:24.078514099 CET	8.8.8.8	192.168.2.7	0xef52	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49723	216.146.43.70	80	C:\Users\user\Desktop\ST_PLC URGENT ORDER 0223308737,pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:38:20.967432022 CET	971	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Feb 23, 2021 17:38:21.041201115 CET	972	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.38</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49724	216.146.43.70	80	C:\Users\user\Desktop\ST_PLC URGENT ORDER 0223308737,pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:38:21.311459064 CET	976	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:38:21.387928963 CET	976	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.38</body></html>

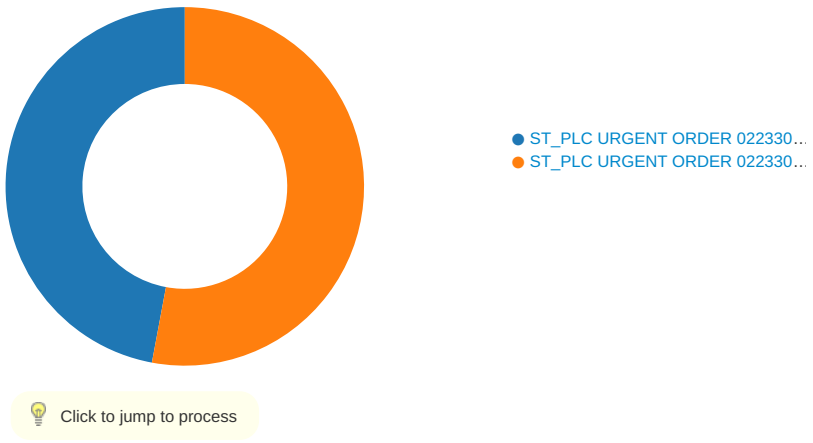
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 17:38:24.243105888 CET	104.21.19.200	443	192.168.2.7	49726	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020	Tue Aug 10 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ST_PLC URGENT ORDER 0223308737,pdf.exe PID: 6256 Parent PID: 5708

General

Start time:	17:37:36
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\ST_PLC URGENT ORDER 0223308737,pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ST_PLC URGENT ORDER 0223308737,pdf.exe'
Imagebase:	0x7fffae0c0000
File size:	451584 bytes
MD5 hash:	49B05DE1926BE1EA5993874AD14C8D3A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.326366120.0000000003651000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.326366120.0000000003651000.00000004.00000001.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	6D4DCF06	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	6D4DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ST_PLC URGENT ORDER 0223308737,pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D7EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ST_PLC URGENT ORDER 0223308737,pdf.exe.log	unknown	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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.Windows.Forms, Vers	success or wait	1	6D7EC907	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	6D4B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D4B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D4B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C321B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C321B4F	ReadFile

Analysis Process: ST_PLC URGENT ORDER 0223308737,pdf.exe PID: 5656 Parent PID: 6256

General

Start time:	17:38:18
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\ST_PLC URGENT ORDER 0223308737,pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7fffae0c0000
File size:	451584 bytes
MD5 hash:	49B05DE1926BE1EA5993874AD14C8D3A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000009.00000002.502527744.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000009.00000002.502527744.0000000000402000.00000040.00000001.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	6D4DCF06	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	6D4DCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6C326A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6C326A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6C326A95	DeleteFileW

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	6D4B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D4B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D4B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D4B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C321B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C321B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C321B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis