ID: 715160
Sample Name: PIptrFxrxR.exe
Cookbook: default.jbs
Time: 17:32:07
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

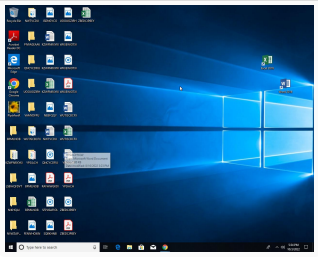
Windows Analysis Report

PlptrFxrxR.exe

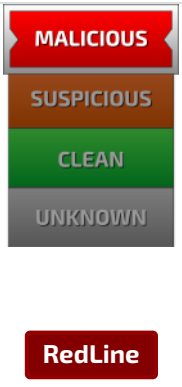
Overview

General Information

Sample Name:	PlptrFxrxR.exe
Analysis ID:	715160
MD5:	3570cfa79638c1…
SHA1:	205fcd2a3a45d9..
SHA256:	5b82bbf81826faa.
Tags:	exe RedLineStealer
Infos:	



Detection



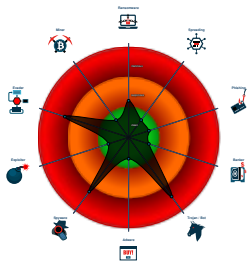
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Snort IDS alert for network traffic
- Queries sensitive video device infor…
- Tries to steal Crypto Currency Walle…
- Queries sensitive disk information (v…
- Machine Learning detection for sam…
- Tries to harvest and steal browser in…
- Creates a DirectInput object (often f…
- Is looking for software installed on t…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- PlptrFxrxR.exe (PID: 3804 cmdline: C:\Users\user\Desktop\PlptrFxrxR.exe MD5: 3570CFA79638C148588F3F22A7AD58C9)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "65.108.247.147:37767"
  ],
  "Authorization Header": "6a82f1fb90afb278c299e83d46279927"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
PlptrFxrxR.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1c68:$pat14: , CommandLine: • 0x39a2b:$v2_1: ListOfProcesses • 0x397b4:$v4_3: base64str • 0x3a8c2:$v4_4: stringKey • 0x3729f:$v4_5: BytesToStringConverted • 0x362e6:$v4_6: FromBase64 • 0x37a9b:$v4_8: procName • 0x37e38:$v5_1: DownloadAndExecuteUpdate • 0x396c4:$v5_2: ITaskProcessor • 0x37e26:$v5_3: CommandLineUpdate • 0x37e17:$v5_4: DownloadUpdate • 0x3853f:$v5_5: FileScanning • 0x3761e:$v5_7: RecordHeaderField • 0x3700c:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: PlptrFxrxR.exe PID: 3804	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: PlptrFxrxR.exe PID: 3804	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.PlptrFxrxR.exe.990000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1c68:$pat14: , CommandLine: • 0x39a2b:$v2_1: ListOfProcesses • 0x397b4:$v4_3: base64str • 0x3a8c2:$v4_4: stringKey • 0x3729f:$v4_5: BytesToStringConverted • 0x362e6:$v4_6: FromBase64 • 0x37a9b:$v4_8: procName • 0x37e38:$v5_1: DownloadAndExecuteUpdate • 0x396c4:$v5_2: ITaskProcessor • 0x37e26:$v5_3: CommandLineUpdate • 0x37e17:$v5_4: DownloadUpdate • 0x3853f:$v5_5: FileScanning • 0x3761e:$v5_7: RecordHeaderField • 0x3700c:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.5 - Destination IP: 65.108.247.147

Timestamp:	192.168.2.565.108.247.14749698377672850027 10/03/22-17:33:23.343299
SID:	2850027
Source Port:	49698
Destination Port:	37767
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.108.247.147	
Timestamp:	192.168.2.565.108.247.14749698377672850286 10/03/22-17:33:45.506493
SID:	2850286
Source Port:	49698
Destination Port:	37767
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 65.108.247.147 - Destination IP: 192.168.2.5	
Timestamp:	65.108.247.147192.168.2.537767496982850353 10/03/22-17:33:24.983524
SID:	2850353
Source Port:	37767
Destination Port:	49698
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)

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

Remote Access Functionality

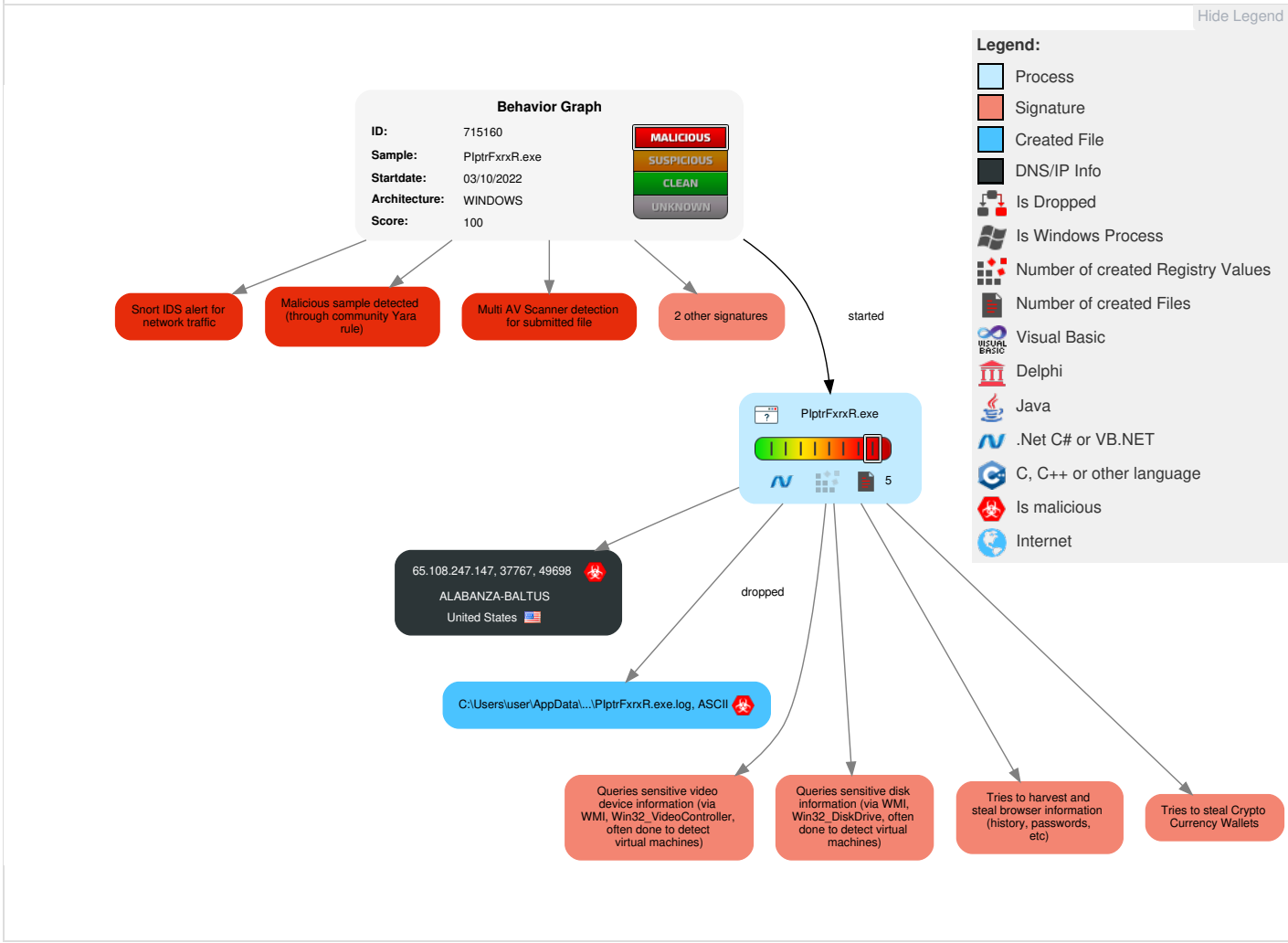
Yara detected RedLine Stealer

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

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 2 1 Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	1 OS Credential Dumping	2 3 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	1 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)	2 3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 2 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

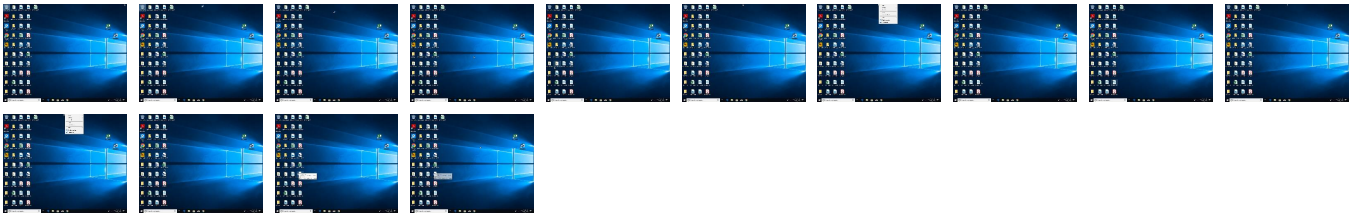
Behavior Graph



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
PlptrFxrxR.exe	81%	ReversingLabs	ByteCode-MSIL.Infostealer.RedLine	
PlptrFxrxR.exe	66%	Virustotal		Browse
PlptrFxrxR.exe	61%	Metadefender		Browse
PlptrFxrxR.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	PIptrFxrxR.exe, 00000000.00000002.398595426.0000000003124000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.399235681.000000000321E000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.399542263.000000000328F000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.400059135.000000000332B000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.402706969.0000000003EF0000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.401620836.00000000034BF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	PIptrFxrxR.exe, 00000000.00000002.402706969.0000000003EF0000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.401620836.00000000034BF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	PIptrFxrxR.exe, 00000000.00000002.396395728.000000000151E000.00000004.00000020.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000003.392866445.000000000151C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high

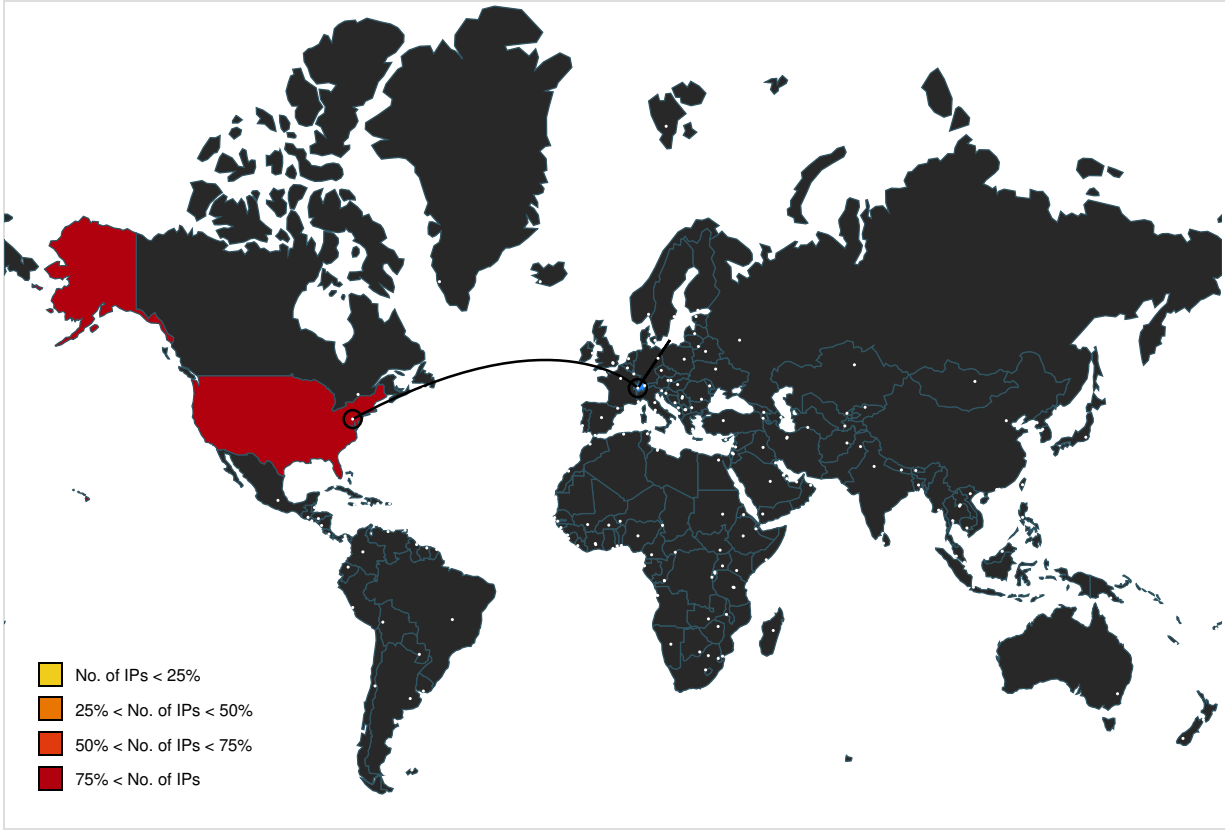
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/faulth	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PIptrFxrxR.exe, 00000000.00000002.397506308.0000000002F99000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	PIptrFxrxR.exe, 00000000.00000002.401721951.00000000034CC000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	PIptrFxrxR.exe, 00000000.00000002.402706969.0000000003EF0000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.401620836.00000000034BF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	PIptrFxrxR.exe, 00000000.00000002.398595426.0000000003124000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.399235681.000000000321E000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.399542263.000000000328F000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.400059135.000000000332B000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.402706969.0000000003EF0000.00000004.00000800.00020000.00000000.sdmp, PIptrFxrxR.exe, 00000000.00000002.401620836.00000000034BF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	PIptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	PIptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.397506308.0000000002F99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	PlptrFxrxR.exe, 00000000.00000002.397506308.0000000002F99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.397506308.0000000002F99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.397506308.0000000002F99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	PlptrFxrxR.exe, 00000000.00000002.398595426.0000000003124000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.399235681.000000000321E000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.399542263.000000000328F000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.400059135.000000000332B000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.402706969.0000000003EF0000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.401620836.00000000034BF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23Response	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.396923501.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp, PlptrFxrxR.exe, 00000000.00000002.397506308.0000000002F99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	PlptrFxrxR.exe, 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.108.247.147	unknown	United States		11022	ALABANZA-BALTUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715160
Start date and time:	2022-10-03 17:32:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PIptrFxrxR.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	3
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@1/1@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:33:42	API Interceptor	26x Sleep call for process: PIptrFxrxR.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\PIptrFxrxR.exe.log

Process:	C:\Users\user\Desktop\PIptrFxrxR.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHK1HjHK0:iqXeqm00YqhQnouOqLqdqNq2qzcGtlxY
MD5:	9A010D404524B7E80B293AEC6FB4AF7F
SHA1:	B238A081C1D05DA6F76DA2F30C529C4275CCF5CF
SHA-256:	3FF08BA477214E6F51EC1F879A44FC02CBE69A69B072E7B317F337A786B21D63
SHA-512:	C7D0D118BFF6E2EDEF02290FC042556502D99967A37A5EDF98AF905BA66C4C2D2C159594DB3D22B5117EC5AA7DB910313A6370F650B9534D5B17E57378E02E2A
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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.04482516274698
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PIptrFxrxR.exe
File size:	369152
MD5:	3570cfa79638c148588f3f22a7ad58c9
SHA1:	205fcd2a3a45d91ee1bdbaf820f49967539e0159
SHA256:	5b82bbf81826faa8e2ff41c468af4632d3151eabec01e5535d9a7c4659528c51
SHA512:	2dba3f1abfea0fe86fbf9581953528b02e88f96f45d2a22092bbc5d3922cb7540843d61758b3ee10dd57af70b38119dbfd1868df6d910562f607ed99f328144a
SSDEEP:	6144:tJhbp5Iy4wUHkjT/eASp1+7lvoe/YuasdHQO33JnTyIuHOn4ssEFZlQ3uSwsZ5jY:vhf+DMTmASP+uewuasdHQO33JnTyIuHZ
TLSH:	6074619D766072EFC857C976CAA81C64FA7074BB930BD203A06316ED9A4D59BCF140F2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....>.... .....@.. .....@.....

File Icon

Icon Hash:	5161454747646c1b

Static PE Info

General

Entrypoint:	0x45b13e
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:	0xF5E7E28F [Sun Sep 26 04:05:35 2100 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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0x5b0f0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5c000	0xab2	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x59144	0x59200	False	0.45041308730715285	data	6.051994541490018	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x5c000	0xab2	0xc00	False	0.5511067708333334	data	5.137865378285585	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	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_ICON	0x5c130	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 2834 x 2834 px/m		
RT_GROUP_ICON	0x5c598	0x14	data		
RT_VERSION	0x5c5ac	0x31c	data		
RT_MANIFEST	0x5c8c8	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
192.168.2.565.108.247.147496983776728500710/03/22-17:33:23.343299	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49698	37767	192.168.2.5	65.108.247.147
192.168.2.565.108.247.147496983776728502810/03/22-17:33:45.506493	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49698	37767	192.168.2.5	65.108.247.147
65.108.247.147192.168.2.537767496982850353 10/03/22-17:33:24.983524	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	37767	49698	65.108.247.147	192.168.2.5

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:33:22.906542063 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:22.944623947 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:22.947901964 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:23.343298912 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:23.382127047 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:23.605457067 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:24.941049099 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:24.983524084 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:25.105386972 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:32.487346888 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:32.535263062 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:32.535300970 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:32.535320044 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:32.535408974 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:34.352969885 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:34.395081997 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:34.449945927 CEST	49698	37767	192.168.2.5	65.108.247.147

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:33:35.018985987 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.075258970 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:35.086642027 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.168145895 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:35.311141014 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:35.356277943 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.398336887 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.437460899 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:35.481300116 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.570745945 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.609148026 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:35.635761023 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.674354076 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:35.686705112 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:35.725313902 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:35.778151989 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:36.019516945 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:36.057555914 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:36.058671951 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:36.106349945 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:36.236470938 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:36.274313927 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:36.274352074 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:36.274367094 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:36.275789022 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:36.295092106 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:36.333673954 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:36.387658119 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:37.009210110 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:37.051856041 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:37.106440067 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:37.606472969 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:37.644608021 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:37.645085096 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:37.700344086 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:37.736826897 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:37.775484085 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:37.825210094 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.185143948 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.226258993 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.278942108 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.489326000 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.527784109 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.669680119 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.873816967 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.911992073 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.912024975 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.912050009 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.912126064 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.912170887 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.912221909 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.912324905 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.912358046 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.951165915 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.951196909 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.951209068 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.951220989 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.951235056 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.951248884 CEST	37767	49698	65.108.247.147	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:33:44.951263905 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.951276064 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.951431036 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.951517105 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.951766968 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.989597082 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.989684105 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.989763975 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.989778996 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.989813089 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.989828110 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.989897013 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.989980936 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990366936 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990389109 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990406036 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990422964 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990441084 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990453959 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990524054 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.990648031 CEST	49698	37767	192.168.2.5	65.108.247.147
Oct 3, 2022 17:33:44.990686893 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990700006 CEST	37767	49698	65.108.247.147	192.168.2.5
Oct 3, 2022 17:33:44.990734100 CEST	37767	49698	65.108.247.147	192.168.2.5

Statistics

No statistics

System Behavior

Analysis Process: PlptrFxrxR.exe PID: 3804, Parent PID: 3324

General

Target ID:	0
Start time:	17:33:01
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\PlptrFxrxR.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PlptrFxrxR.exe
Imagebase:	0x990000
File size:	369152 bytes
MD5 hash:	3570CFA79638C148588F3F22A7AD58C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.397297996.0000000002F54000.00000004.00000800.00020000.00000000.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	6CBBCF06	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	6CBBCF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BA0BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BA0BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PIptrFxrxR.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CECC78D	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\PIptrFxrxR.exe.log	0	2843	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 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	6CECC907	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	6CB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CB95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CAF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CB9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6CAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6CAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6CAF03DE	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	6CAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6CAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CAF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CAF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CB95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\KZWFNRXYKI.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\KZWFNRXYKI.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	4096	success or wait	1	6BA01B4F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	1022	end of file	1	6BA01B4F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	114	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	7	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6BA01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	131	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	8	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	71	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6BA01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6BA01B4F	ReadFile

Disassembly

No disassembly