ID: 756117
Sample Name: SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe
Cookbook: default.jbs
Time: 16:49:18
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Lokibot 4
Yara Signatures 4
PCAP (Network Traffic) 4
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 19
AV Detection 19
Networking 19
System Summary 19
Data Obfuscation 19
HIPS / PFW / Operating System Protection Evasion 19
Stealing of Sensitive Information 19
Mitre Att&ck Matrix 19
Behavior Graph 20
Screenshots 21
Thumbnails 21
Antivirus, Machine Learning and Genetic Malware Detection 22
Initial Sample 22
Dropped Files 22
Unpacked PE Files 22
Domains 23
URLs 23
Domains and IPs 23
Contacted Domains 23
Contacted URLs 23
URLs from Memory and Binaries 23
World Map of Contacted IPs 26
Public IPs 26
Private 26
General Information 27
Warnings 27
Simulations 27
Behavior and APIs 27
Joe Sandbox View / Context 28
IPs 28
Domains 28
ASNs 28
JA3 Fingerprints 28
Dropped Files 28
Created / dropped Files 28
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.log 28
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 28
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 29
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_150mte30.zn5.psm1 29
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cdh4roqr.3j3.psm1 29
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hojog3ew.0sb.ps1 29
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kk3bso0d.u4o.ps1 30
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck 30
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a 30
Static File Info 31
General 31
File Icon 31
Static PE Info 31
General 31
Entrypoint Preview 31
Data Directories 33
Sections 33
Resources 34
Imports 34
Network Behavior 34

Snort IDS Alerts 34
Network Port Distribution 39
TCP Packets 40
UDP Packets 42
DNS Queries 42
DNS Answers 43
HTTP Request Dependency Graph 44
Statistics 44
Behavior 44
System Behavior 44
Analysis Process: SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exePID: 5092, Parent PID: 3320 44
General 45
File Activities 45
File Created 45
File Written 45
File Read 46
Registry Activities 46
Analysis Process: powershell.exePID: 1508, Parent PID: 5092 46
General 46
File Activities 47
File Created 47
File Deleted 47
File Written 47
File Read 49
Analysis Process: conhost.exePID: 5700, Parent PID: 1508 50
General 50
Analysis Process: svchost.exePID: 2084, Parent PID: 552 51
General 51
Analysis Process: powershell.exePID: 1376, Parent PID: 5092 51
General 51
File Activities 51
File Created 51
File Deleted 52
File Written 52
File Read 53
Analysis Process: conhost.exePID: 5096, Parent PID: 1376 54
General 54
Analysis Process: RegAsm.exePID: 2084, Parent PID: 5092 54
General 54
File Activities 54
File Created 54
File Deleted 55
File Moved 55
File Written 55
File Read 55
Disassembly 55

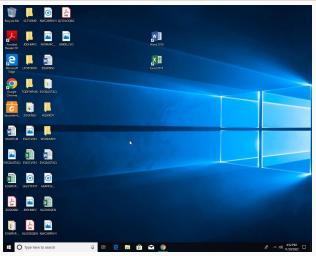
Windows Analysis Report

SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe

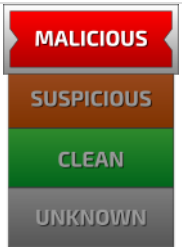
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe
Analysis ID:	756117
MD5:	3039fa7b347872..
SHA1:	69832bbe446653.
SHA256:	f949fda96d4810c..
Tags:	exe
Infos:	



Detection



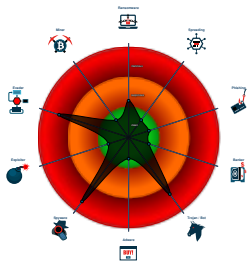
Lokibot

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected Lokibot
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…
- Tries to harvest and steal ftp login c…
- Encrypted powershell cmdline option…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe (PID: 5092 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe MD5: 3039FA7B347872C33C247581A27A7560)
  - powershell.exe (PID: 1508 cmdline: "powershell" Get-Date MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - svchost.exe (PID: 2084 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - powershell.exe (PID: 1376 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 2084 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: Lokibot

```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "http://sedesadre.gq/PKZ/PWS/fre.php"
  ]
}
```

Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.521369809.0000000003243000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x437f:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6
00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x17f10:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.4291b00.0.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13e80:$s2: https:// • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
0.2.SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.4291b00.0.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.4291b00.0.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.4291b00.0.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
0.2.SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.4291b00.0.raw.unpack	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x16536:$f1: FileZilla\recentservers.xml • 0x16576:$f2: FileZilla\sitemanager.xml • 0x147e6:$b2: Mozilla\Firefox\Profiles • 0x14550:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x146fa:$s4: logins.json • 0x155a4:$s6: wand.dat • 0x14024:$a1: username_value • 0x14014:$a2: password_value • 0x1465f:$a3: encryptedUsername • 0x146cc:$a3: encryptedUsername • 0x14672:$a4: encryptedPassword • 0x146e0:$a4: encryptedPassword
Click to see the 34 entries				

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102 −

Timestamp:	192.168.2.7141.98.6.10249731802021641 11/29/22-16:52:33.757391
SID:	2021641
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249720802025381 11/29/22-16:52:28.227779
SID:	2025381
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249717802025381 11/29/22-16:52:26.668343
SID:	2025381
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249726802025381 11/29/22-16:52:31.339365
SID:	2025381
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249725802024313 11/29/22-16:52:30.920170
SID:	2024313
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249725802024318 11/29/22-16:52:30.920170
SID:	2024318
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249716802024317 11/29/22-16:52:25.029133
SID:	2024317
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249722802021641 11/29/22-16:52:29.504056
SID:	2021641
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249716802024312 11/29/22-16:52:25.029133
SID:	2024312
Source Port:	49716

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

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249718802825766 11/29/22-16:52:27.285136
SID:	2825766
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249719802021641 11/29/22-16:52:27.785438
SID:	2021641
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249727802825766 11/29/22-16:52:31.817491
SID:	2825766
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249721802825766 11/29/22-16:52:28.704063
SID:	2825766
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249730802825766 11/29/22-16:52:33.273429
SID:	2825766
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249728802021641 11/29/22-16:52:32.198993
SID:	2021641
Source Port:	49728
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249730802025381 11/29/22-16:52:33.273429
SID:	2025381
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249721802021641 11/29/22-16:52:28.704063
SID:	2021641
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249727802021641 11/29/22-16:52:31.817491
SID:	2021641
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249717802825766 11/29/22-16:52:26.668343
SID:	2825766
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249732802021641 11/29/22-16:52:36.325135
SID:	2021641
Source Port:	49732
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497182025483 11/29/22-16:52:27.393637
SID:	2025483
Source Port:	80
Destination Port:	49718
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249718802025381 11/29/22-16:52:27.285136
SID:	2025381
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249728802825766 11/29/22-16:52:32.198993
SID:	2825766
Source Port:	49728
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497212025483 11/29/22-16:52:28.798694
SID:	2025483
Source Port:	80

Destination Port:	49721
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497202025483 11/29/22-16:52:28.346106
SID:	2025483
Source Port:	80
Destination Port:	49720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249717802024312 11/29/22-16:52:26.668343
SID:	2024312
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249726802021641 11/29/22-16:52:31.339365
SID:	2021641
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249723802024318 11/29/22-16:52:30.023507
SID:	2024318
Source Port:	49723
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249720802024318 11/29/22-16:52:28.227779
SID:	2024318
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497242025483 11/29/22-16:52:30.593492
SID:	2025483
Source Port:	80
Destination Port:	49724
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497252025483 11/29/22-16:52:31.018575
SID:	2025483
Source Port:	80
Destination Port:	49725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249731802025381 11/29/22-16:52:33.757391
SID:	2025381
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249722802025381 11/29/22-16:52:29.504056
SID:	2025381
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249717802024317 11/29/22-16:52:26.668343
SID:	2024317
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249723802024313 11/29/22-16:52:30.023507
SID:	2024313
Source Port:	49723
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249716802025381 11/29/22-16:52:25.029133
SID:	2025381
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249719802025381 11/29/22-16:52:27.785438
SID:	2025381
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249720802024313 11/29/22-16:52:28.227779
SID:	2024313
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249725802025381 11/29/22-16:52:30.920170
SID:	2025381
Source Port:	49725

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

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249726802825766 11/29/22-16:52:31.339365
SID:	2825766
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249718802021641 11/29/22-16:52:27.285136
SID:	2021641
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249732802825766 11/29/22-16:52:36.325135
SID:	2825766
Source Port:	49732
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249727802025381 11/29/22-16:52:31.817491
SID:	2025381
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497282025483 11/29/22-16:52:32.293466
SID:	2025483
Source Port:	80
Destination Port:	49728
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249729802021641 11/29/22-16:52:32.689634
SID:	2021641
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249730802021641 11/29/22-16:52:33.273429
SID:	2021641
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249724802021641 11/29/22-16:52:30.488585
SID:	2021641
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249731802024313 11/29/22-16:52:33.757391
SID:	2024313
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249722802024318 11/29/22-16:52:29.504056
SID:	2024318
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249725802021641 11/29/22-16:52:30.920170
SID:	2021641
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249728802024318 11/29/22-16:52:32.198993
SID:	2024318
Source Port:	49728
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249719802024318 11/29/22-16:52:27.785438
SID:	2024318
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249732802025381 11/29/22-16:52:36.325135
SID:	2025381
Source Port:	49732
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249731802024318 11/29/22-16:52:33.757391
SID:	2024318
Source Port:	49731

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

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249723802025381 11/29/22-16:52:30.023507
SID:	2025381
Source Port:	49723
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249722802024313 11/29/22-16:52:29.504056
SID:	2024313
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249719802024313 11/29/22-16:52:27.785438
SID:	2024313
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249716802021641 11/29/22-16:52:25.029133
SID:	2021641
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	−
Timestamp:	141.98.6.102192.168.2.780497312025483 11/29/22-16:52:33.852928
SID:	2025483
Source Port:	80
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	−
Timestamp:	141.98.6.102192.168.2.780497302025483 11/29/22-16:52:33.400113
SID:	2025483
Source Port:	80
Destination Port:	49730
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	−
Timestamp:	141.98.6.102192.168.2.780497322025483 11/29/22-16:52:36.428850
SID:	2025483
Source Port:	80
Destination Port:	49732
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249728802024313 11/29/22-16:52:32.198993
SID:	2024313
Source Port:	49728
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249724802825766 11/29/22-16:52:30.488585
SID:	2825766
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249729802825766 11/29/22-16:52:32.689634
SID:	2825766
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249727802024313 11/29/22-16:52:31.817491
SID:	2024313
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249723802825766 11/29/22-16:52:30.023507
SID:	2825766
Source Port:	49723
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249721802024313 11/29/22-16:52:28.704063
SID:	2024313
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249724802025381 11/29/22-16:52:30.488585
SID:	2025381
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249721802024318 11/29/22-16:52:28.704063
SID:	2024318
Source Port:	49721

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

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497272025483 11/29/22-16:52:31.911870
SID:	2025483
Source Port:	80
Destination Port:	49727
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497292025483 11/29/22-16:52:32.805162
SID:	2025483
Source Port:	80
Destination Port:	49729
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249727802024318 11/29/22-16:52:31.817491
SID:	2024318
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249729802025381 11/29/22-16:52:32.689634
SID:	2025381
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249716802825766 11/29/22-16:52:25.029133
SID:	2825766
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249719802825766 11/29/22-16:52:27.785438
SID:	2825766
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249725802825766 11/29/22-16:52:30.920170
SID:	2825766
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249717802021641 11/29/22-16:52:26.668343
SID:	2021641
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497222025483 11/29/22-16:52:29.613062
SID:	2025483
Source Port:	80
Destination Port:	49722
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249726802024313 11/29/22-16:52:31.339365
SID:	2024313
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249722802825766 11/29/22-16:52:29.504056
SID:	2825766
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497232025483 11/29/22-16:52:30.124555
SID:	2025483
Source Port:	80
Destination Port:	49723
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	
Timestamp:	141.98.6.102192.168.2.780497262025483 11/29/22-16:52:31.441372
SID:	2025483
Source Port:	80
Destination Port:	49726
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249732802024313 11/29/22-16:52:36.325135
SID:	2024313
Source Port:	49732
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249726802024318 11/29/22-16:52:31.339365
SID:	2024318
Source Port:	49726

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

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	▬
Timestamp:	192.168.2.7141.98.6.10249728802025381 11/29/22-16:52:32.198993
SID:	2025381
Source Port:	49728
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	▬
Timestamp:	192.168.2.7141.98.6.10249723802021641 11/29/22-16:52:30.023507
SID:	2021641
Source Port:	49723
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	▬
Timestamp:	192.168.2.7141.98.6.10249732802024318 11/29/22-16:52:36.325135
SID:	2024318
Source Port:	49732
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	▬
Timestamp:	192.168.2.7141.98.6.10249720802021641 11/29/22-16:52:28.227779
SID:	2021641
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	▬
Timestamp:	192.168.2.7141.98.6.10249718802024318 11/29/22-16:52:27.285136
SID:	2024318
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 141.98.6.102 - Destination IP: 192.168.2.7	▬
Timestamp:	141.98.6.102192.168.2.780497192025483 11/29/22-16:52:27.888790
SID:	2025483
Source Port:	80
Destination Port:	49719
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	▬
Timestamp:	192.168.2.7141.98.6.10249729802024318 11/29/22-16:52:32.689634
SID:	2024318
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249731802825766 11/29/22-16:52:33.757391
SID:	2825766
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249729802024313 11/29/22-16:52:32.689634
SID:	2024313
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249730802024318 11/29/22-16:52:33.273429
SID:	2024318
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249730802024313 11/29/22-16:52:33.273429
SID:	2024313
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249721802025381 11/29/22-16:52:28.704063
SID:	2025381
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249724802024318 11/29/22-16:52:30.488585
SID:	2024318
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249718802024313 11/29/22-16:52:27.285136
SID:	2024313
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	
Timestamp:	192.168.2.7141.98.6.10249720802825766 11/29/22-16:52:28.227779
SID:	2825766
Source Port:	49720

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

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.7 - Destination IP: 141.98.6.102	−
Timestamp:	192.168.2.7141.98.6.10249724802024313 11/29/22-16:52:30.488585
SID:	2024313
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected aPLib compressed binary

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Lokibot

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

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

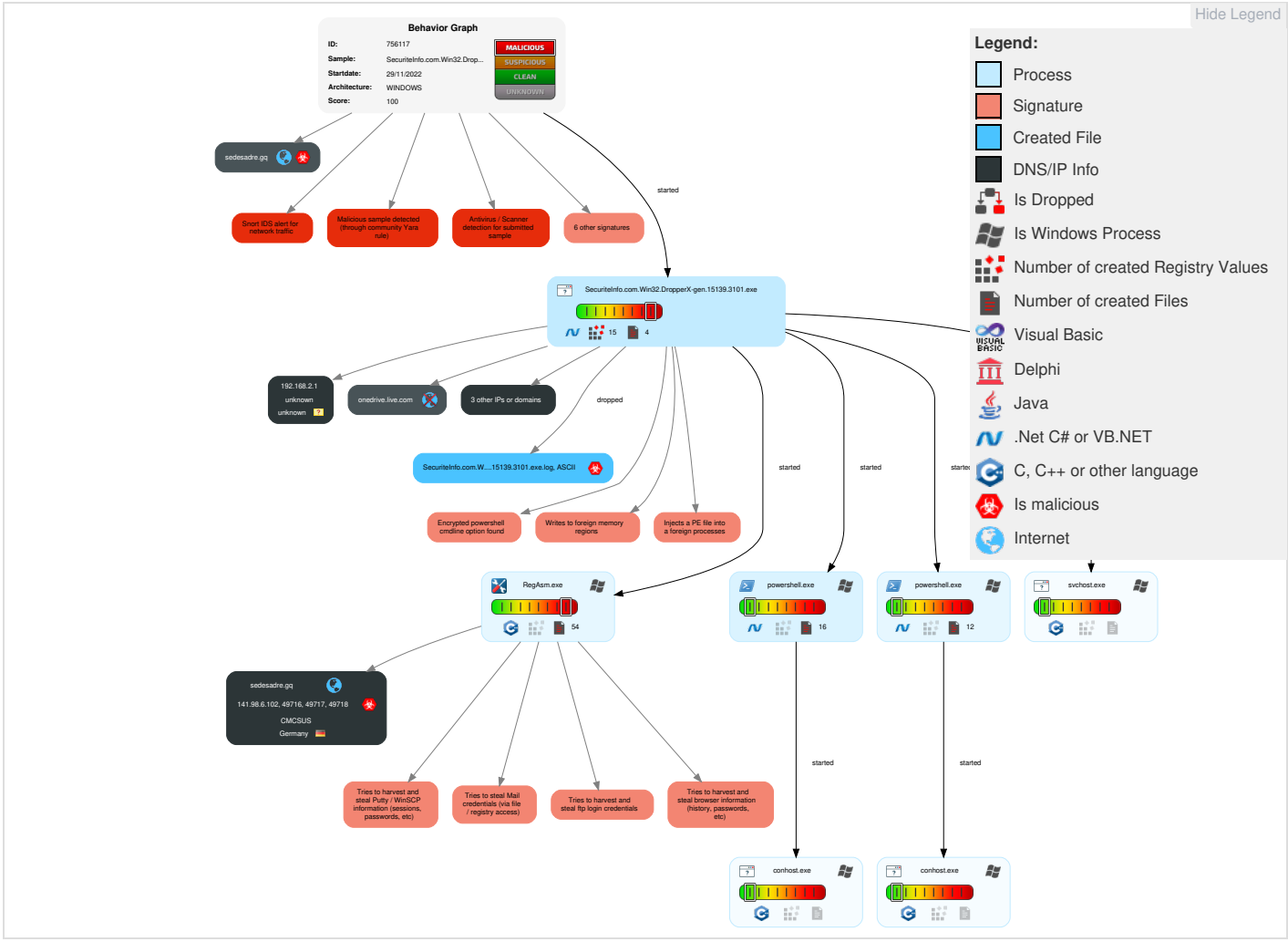
Tries to harvest and steal ftp login credentials

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 PowerShell	1 DLL Side-Loading	2 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 1 2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 1 Process Injection	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 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

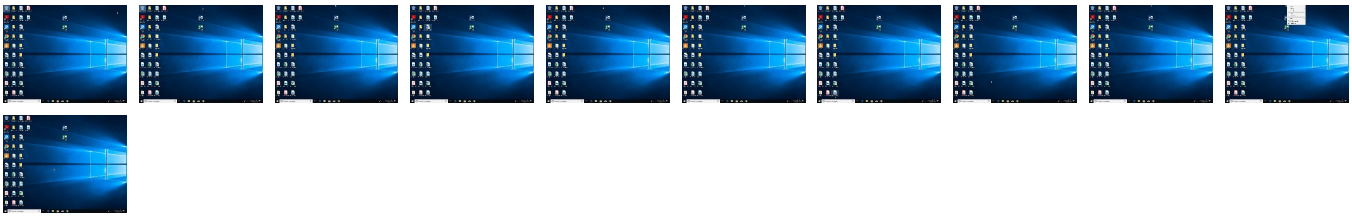
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe	15%	ReversingLabs	ByteCode-MSIL.Trojan.Bsymem	
SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe	100%	Avira	HEUR/AGEN.1202504	
SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.42b9b20.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.4291b00.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://edi4gw.db.files.1drv.com4	0%	Avira URL Cloud	safe	
http://sedesadre.gq/PKZ/PWS/fre.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l-0003.l-dc-msedge.net	13.107.43.12	true	false		unknown
sedesadre.gq	141.98.6.102	true	true		unknown
onedrive.live.com	unknown	unknown	false		high
edi4gw.db.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sedesadre.gq/PKZ/PWS/fre.php	true	• Avira URL Cloud: safe	unknown
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

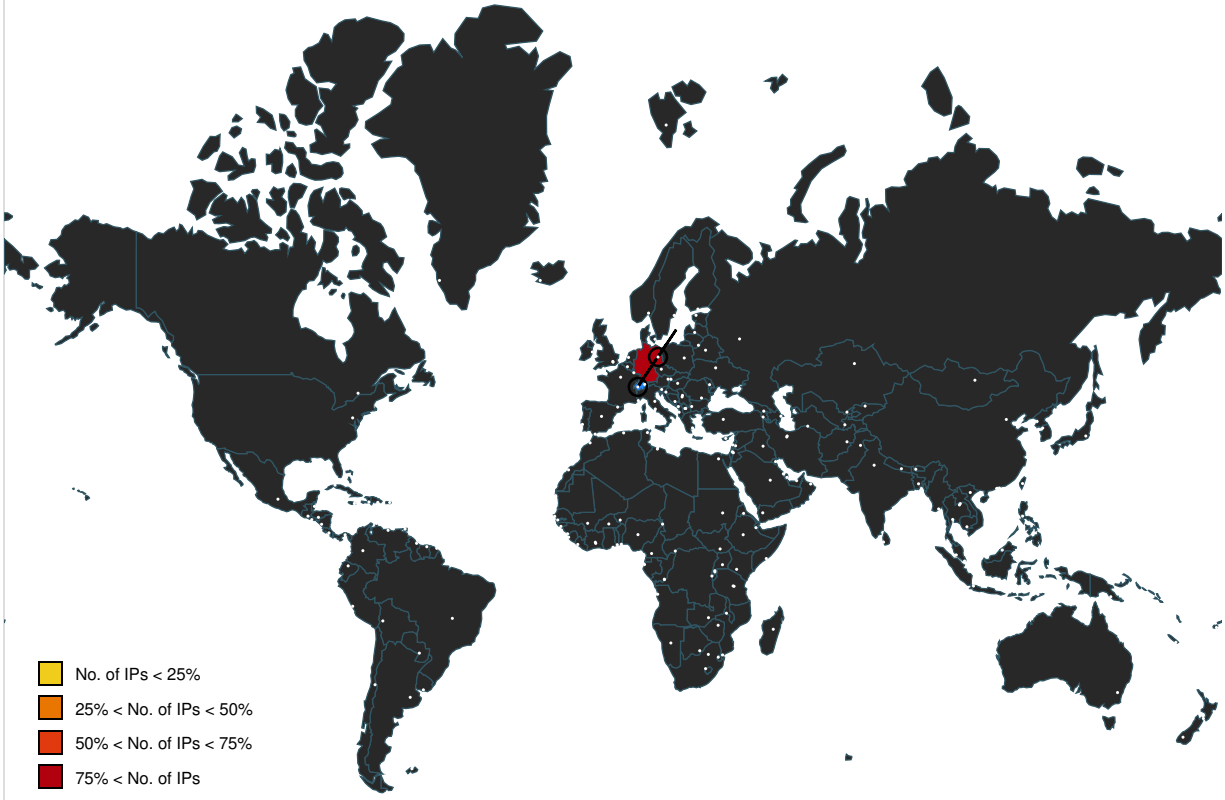
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://edi4gw.db.files.1drv.com4	SecuriteInfo.com.Win32.DropperX-gen.1513 9.3101.exe, 00000000.00000002.519404605. 00000000030D1000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000005.00000002.321088494 .0000014604A3C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000005.00000003.319788458 .0000014604A5F000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen .ashx	svchost.exe, 00000005.00000002.321088494 .0000014604A3C000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ibsensoftware.com/	SecuriteInfo.com.Win32.DropperX-gen.1513 9.3101.exe, 00000000.00000002.528024280. 00000000042B9000.00000004.00000800.00020 000.00000000.sdmp, SecuriteInfo.com.Win3 2.DropperX-gen.15139.3101.exe, 00000000. 00000002.521045812.0000000003211000.0000 0004.00000800.00020000.00000000.sdmp, Se curiteInfo.com.Win32.DropperX-gen.15139.3101.exe, 00000000.00000002.527878465.000000000429 1000.00000004.00000800.00020000.00000000.sdmp, RegAsm.exe, 0000000E.00000000.513552356.000 0000000415000.00000040.00000400.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000005.00000003.319889828 .0000014604A59000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000002.321240546.0000014604A5C000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000005.00000002.321163191 .0000014604A4E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000003.319680997.0000014604A48000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000001.00000002.423054 874.00000000059BE000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000005.00000003.319788458 .0000014604A5F000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://onedrive.live.com/download?cid=9A063D4B0D931024&resid=9A063D4B0D931024%21128&authkey=AFWFoMk	SecuriteInfo.com.Win32.DropperX-gen.1513 9.3101.exe	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000005.00000003.319937311 .0000014604A40000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000002.321132883.0000014604A42000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000005.00000003.319788458 .0000014604A5F000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000005.00000003.319889828 .0000014604A59000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000005.00000003.297637720 .0000014604A31000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000005.00000003.319937311 .0000014604A40000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000002.321132883.0000014604A42000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000001.00000002.423054 874.00000000059BE000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000001.00000002.423054 874.00000000059BE000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.DropperX-gen.1513 9.3101.exe, 00000000.00000002.518826525. 0000000003087000.00000004.00000800.00020 000.00000000.sdmp, powershell.exe, 00000 001.00000002.401922859.0000000004961000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000005.00000002.320847106 .0000014604A13000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000005.00000002.321088494 .0000014604A3C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000005.00000003.319788458 .0000014604A5F000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000001.00000002.423054 874.00000000059BE000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000005.00000002.321224479 .0000014604A55000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000001.00000002.404488163.0000000004A9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com	SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe, 00000000.00000002.518826525.0000000003087000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000001.00000002.404488163.0000000004A9B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000001.00000002.420135572.00000000051CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000005.00000002.321088494.0000014604A3C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/download?cid=9A063D4B0D931024&resid=9A063D4B0D931024	SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe, 00000000.00000002.518826525.0000000003087000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000001.00000002.423054874.00000000059BE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000005.00000003.297637720.0000014604A31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000005.00000003.319937311.0000014604A40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000003.319889828.0000014604A59000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000002.321240546.0000014604A5C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000005.00000002.321088494.0000014604A3C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000002.320944817.0000014604A27000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000005.00000002.321163191.0000014604A4E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000003.319680997.0000014604A48000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000005.00000003.319788458.0000014604A5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000005.00000003.297637720.0000014604A31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000005.00000003.319788458.0000014604A5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000001.00000002.404488163.0000000004A9B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe, 00000000.00000002.521644432.000000000327E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe, 00000000.00000002.519732360.0000000003147000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000005.00000003.319889828.0000014604A59000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000002.321240546.0000014604A5C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000005.00000003.319889828.0000014604A59000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000002.321240546.0000014604A5C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000005.00000003.319680997.0000014604A48000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000005.00000003.319788458.0000014604A5F000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.newtonsoft.com/jsonschema	SecuriteInfo.com.Win32.DropperX-gen.1513 9.3101.exe, 00000000.00000002.531258657. 0000000006C30000.00000004.08000000.00040 000.00000000.sdmp, SecuriteInfo.com.Win3 2.DropperX-gen.15139.3101.exe, 00000000. 00000003.490102974.00000000045F2000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000005.00000003.297637720 .0000014604A31000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000002.321064418.0000014604A3A000.00 000004.00000020.00020000.00000000.sdmp	false		high
http:// https://www.nuget.org/packages/Newtonsoft.Json.Bso n	SecuriteInfo.com.Win32.DropperX-gen.1513 9.3101.exe, 00000000.00000002.531258657. 0000000006C30000.00000004.08000000.00040 000.00000000.sdmp, SecuriteInfo.com.Win3 2.DropperX-gen.15139.3101.exe, 00000000. 00000003.490102974.00000000045F2000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv? pv=1&r=	svchost.exe, 00000005.00000003.319889828 .0000014604A59000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000002.321240546.0000014604A5C000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000005.00000003.319788458 .0000014604A5F000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMa ps/data/	svchost.exe, 00000005.00000003.319889828 .0000014604A59000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000002.321240546.0000014604A5C000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd? pv=1&r=	svchost.exe, 00000005.00000003.319889828 .0000014604A59000.00000004.00000020.0002 0000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
141.98.6.102	sedesadre.gq	Germany		33657	CMCSUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756117
Start date and time:	2022-11-29 16:49:18 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.DropperX-gen.15139.3101.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:	15
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@10/9@21/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.13, 13.107.42.12
- Excluded domains from analysis (whitelisted): l-0004.l-msedge.net, odc-web-brs.onedrive.akadns.net, client.wns.windows.com, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, fs.microsoft.com, l-0003.l-msedge.net, odc-web-geo.onedrive.akadns.net, db-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, odc-db-files-geo.onedrive.akadns.net, odc-db-files-brs.onedrive.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe

Simulations

Behavior and APIs

Time	Type	Description
16:51:09	API Interceptor	68x Sleep call for process: powershell.exe modified
16:52:23	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe modified
16:52:27	API Interceptor	14x Sleep call for process: RegAsm.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\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1537
Entropy (8bit):	5.3478589519339295
Encrypted:	false
SSDEEP:	48:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzvFHLHKdHKBqHKs:iqX9qxwCYqhQnoPtIxHeqzNrqdq4qs
MD5:	2A63347CC5F87ABDC744C637814F0C27
SHA1:	4795E5BE85E14E9BDAACB6D00E465F238FA3601F
SHA-256:	F4DCAC81A786946BE4394916C1A88F3C2EDD30660EEC190682793293D38BB865
SHA-512:	961AD4730F9361A6067005AD63EC8828EEA2755EE60754623E0879A2635ADF20BF731900936D555D6422D87AC10318A09A750C03612D12BB2C13815D95FC110E
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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E7

Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.550696665565154
Encrypted:	false
SSDEEP:	384:pte/e27ljK12pCbvlSBxnOulrlSsFvlZA/4oXlYo:LO20B4xOulrYCilo
MD5:	18C379E4374BC2337F9F0D5394A3D7A1
SHA1:	8DEBC168CDEBAF36CAD9ED9DDD69512B742372FB
SHA-256:	4DD8B586651F70808C99483D02E9D19ADB96B728A402FDA3D0DE5D29FDA0936A
SHA-512:	5D1B414DD4F10BE191E64C203706F5BE73F976C971109B39F1483A705C082280B7274CB2FD71B683E6D1DEA4577E668E516ADC4255266BC2B00DDD8254EA813
Malicious:	false
Preview:	@...e..... .....'.....@.....H.....<@.^.L."My...:'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automati on4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....].D.E.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_150mte30.zn5.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cdh4roqr.3j3.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hojog3ew.0sb.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kk3bso0d.u4o.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	50
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	871BDD96B159C14D15C8D97D9111E9C8
SHA1:	8CD537A621659C289F0707BAD94719B5782DDB1F
SHA-256:	CC2786E1F9910A9D811400EDCDDAF7075195F7A16B216DCBEFBA3BC7C4F2AE51
SHA-512:	E116D2D486BC802E99D5FFE83A666D5E324887A65965C7E0D90B238A4EE1DB97E28F59AED23E6F968868902D762DF06146833BE62064C4A74D7C9384DFB0C7F

Malicious:	false
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	3.7691875294894785
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe
File size:	313856
MD5:	3039fa7b347872c33c247581a27a7560
SHA1:	69832bbe446653f7d10eccf07069e73230138af8
SHA256:	f949fda96d4810c4ffa941ecce00160b984cf7ac32cf1ca88dd4dd9583f2e480
SHA512:	175e3f5c4bb39e490c2b25f02e623317923b02f976f7dfc029d0213ca5d3ef2b31deef01fd9a355fdf8d5eea826130e56e45723ab2004d3797de4e11cd4053d2
SSDEEP:	1536:rLc62Vr2beD+oPKjg7cMpdLVPZby1U/r3EVi6DXxhoa:12VCkVUXL
TLSH:	81648E9A9D721284F5154D33E5BBCBA8FB125EA427AD712B2E4C7530063317B2BAF131
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....v4... ...@....@.. ....` .....

File Icon

Icon Hash:	92b21472696d3916

Static PE Info

General

Entrypoint:	0x403476
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385E7BE [Tue Nov 29 11:06:38 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x341c	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x4afcc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x50000	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	0x147c	0x1600	False	0.5161576704545454	data	5.268731127158798	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x4000	0x4afcc	0x4b000	False	0.050693359375	data	3.6559178414965716	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x50000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4220	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 270336		
RT_ICON	0x46248	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896		
RT_ICON	0x4a470	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600		
RT_ICON	0x4ca18	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0x4dac0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400		
RT_ICON	0x4e448	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0x4e8b0	0x5a	data		
RT_VERSION	0x4e90c	0x4bc	data		
RT_MANIFEST	0x4edc8	0x204	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (513), with no 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
192.168.2.7141.98.6.10249731802021641 11/29/22-16:52:33.757391	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49731	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.10249720802025381 11/29/22-16:52:28.227779	TCP	2025381	ET TROJAN LokiBot Checkin	49720	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.10249717802025381 11/29/22-16:52:26.668343	TCP	2025381	ET TROJAN LokiBot Checkin	49717	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.10249726802025381 11/29/22-16:52:31.339365	TCP	2025381	ET TROJAN LokiBot Checkin	49726	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.10249725802024313 11/29/22-16:52:30.920170	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49725	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.10249725802024318 11/29/22-16:52:30.920170	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49725	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.10249716802024317 11/29/22-16:52:25.029133	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49716	80	192.168.2.7	141.98.6.102

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7141.98.6.1024 9722802021641 11/29/22- 16:52:29.504056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49722	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9716802024312 11/29/22- 16:52:25.029133	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49716	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9718802825766 11/29/22- 16:52:27.285136	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49718	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9719802021641 11/29/22- 16:52:27.785438	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49719	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9727802825766 11/29/22- 16:52:31.817491	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49727	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9721802825766 11/29/22- 16:52:28.704063	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49721	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9730802825766 11/29/22- 16:52:33.273429	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49730	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9728802021641 11/29/22- 16:52:32.198993	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49728	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9730802025381 11/29/22- 16:52:33.273429	TCP	2025381	ET TROJAN LokiBot Checkin	49730	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9721802021641 11/29/22- 16:52:28.704063	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49721	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9727802021641 11/29/22- 16:52:31.817491	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49727	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9717802825766 11/29/22- 16:52:26.668343	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49717	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9732802021641 11/29/22- 16:52:36.325135	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49732	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497182025483 11/29/22- 16:52:27.393637	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49718	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9718802025381 11/29/22- 16:52:27.285136	TCP	2025381	ET TROJAN LokiBot Checkin	49718	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9728802825766 11/29/22- 16:52:32.198993	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49728	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497212025483 11/29/22- 16:52:28.798694	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49721	141.98.6.102	192.168.2.7
141.98.6.102192.168.2.78 0497202025483 11/29/22- 16:52:28.346106	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49720	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9717802024312 11/29/22- 16:52:26.668343	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49717	80	192.168.2.7	141.98.6.102

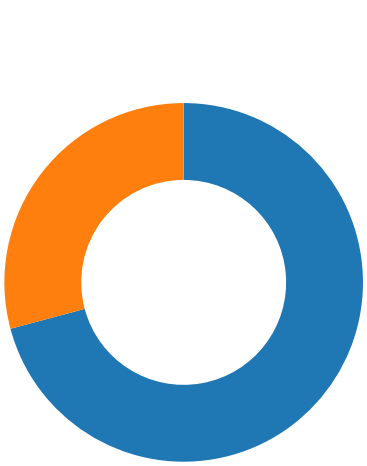
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7141.98.6.1024 9726802021641 11/29/22- 16:52:31.339365	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49726	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9723802024318 11/29/22- 16:52:30.023507	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49723	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9720802024318 11/29/22- 16:52:28.227779	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49720	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497242025483 11/29/22- 16:52:30.593492	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49724	141.98.6.102	192.168.2.7
141.98.6.102192.168.2.78 0497252025483 11/29/22- 16:52:31.018575	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49725	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9731802025381 11/29/22- 16:52:33.757391	TCP	2025381	ET TROJAN LokiBot Checkin	49731	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9722802025381 11/29/22- 16:52:29.504056	TCP	2025381	ET TROJAN LokiBot Checkin	49722	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9717802024317 11/29/22- 16:52:26.668343	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49717	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9723802024313 11/29/22- 16:52:30.023507	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49723	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9716802025381 11/29/22- 16:52:25.029133	TCP	2025381	ET TROJAN LokiBot Checkin	49716	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9719802025381 11/29/22- 16:52:27.785438	TCP	2025381	ET TROJAN LokiBot Checkin	49719	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9720802024313 11/29/22- 16:52:28.227779	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49720	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9725802025381 11/29/22- 16:52:30.920170	TCP	2025381	ET TROJAN LokiBot Checkin	49725	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9726802825766 11/29/22- 16:52:31.339365	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49726	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9718802021641 11/29/22- 16:52:27.285136	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49718	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9732802825766 11/29/22- 16:52:36.325135	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49732	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9727802025381 11/29/22- 16:52:31.817491	TCP	2025381	ET TROJAN LokiBot Checkin	49727	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497282025483 11/29/22- 16:52:32.293466	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49728	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9729802021641 11/29/22- 16:52:32.689634	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49729	80	192.168.2.7	141.98.6.102

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7141.98.6.1024 9730802021641 11/29/22-16:52:33.273429	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49730	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9724802021641 11/29/22-16:52:30.488585	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49724	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9731802024313 11/29/22-16:52:33.757391	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49731	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9722802024318 11/29/22-16:52:29.504056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49722	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9725802021641 11/29/22-16:52:30.920170	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49725	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9728802024318 11/29/22-16:52:32.198993	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49728	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9719802024318 11/29/22-16:52:27.785438	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49719	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9732802025381 11/29/22-16:52:36.325135	TCP	2025381	ET TROJAN LokiBot Checkin	49732	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9731802024318 11/29/22-16:52:33.757391	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49731	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9723802025381 11/29/22-16:52:30.023507	TCP	2025381	ET TROJAN LokiBot Checkin	49723	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9722802024313 11/29/22-16:52:29.504056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49722	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9719802024313 11/29/22-16:52:27.785438	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49719	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9716802021641 11/29/22-16:52:25.029133	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49716	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497312025483 11/29/22-16:52:33.852928	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49731	141.98.6.102	192.168.2.7
141.98.6.102192.168.2.78 0497302025483 11/29/22-16:52:33.400113	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49730	141.98.6.102	192.168.2.7
141.98.6.102192.168.2.78 0497322025483 11/29/22-16:52:36.428850	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49732	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9728802024313 11/29/22-16:52:32.198993	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49728	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9724802825766 11/29/22-16:52:30.488585	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49724	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9729802825766 11/29/22-16:52:32.689634	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49729	80	192.168.2.7	141.98.6.102

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7141.98.6.1024 9727802024313 11/29/22- 16:52:31.817491	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49727	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9723802825766 11/29/22- 16:52:30.023507	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49723	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9721802024313 11/29/22- 16:52:28.704063	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49721	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9724802025381 11/29/22- 16:52:30.488585	TCP	2025381	ET TROJAN LokiBot Checkin	49724	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9721802024318 11/29/22- 16:52:28.704063	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49721	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497272025483 11/29/22- 16:52:31.911870	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49727	141.98.6.102	192.168.2.7
141.98.6.102192.168.2.78 0497292025483 11/29/22- 16:52:32.805162	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49729	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9727802024318 11/29/22- 16:52:31.817491	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49727	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9729802025381 11/29/22- 16:52:32.689634	TCP	2025381	ET TROJAN LokiBot Checkin	49729	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9716802825766 11/29/22- 16:52:25.029133	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49716	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9719802825766 11/29/22- 16:52:27.785438	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49719	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9725802825766 11/29/22- 16:52:30.920170	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49725	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9717802021641 11/29/22- 16:52:26.668343	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49717	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497222025483 11/29/22- 16:52:29.613062	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49722	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9726802024313 11/29/22- 16:52:31.339365	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49726	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9722802825766 11/29/22- 16:52:29.504056	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49722	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497232025483 11/29/22- 16:52:30.124555	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49723	141.98.6.102	192.168.2.7
141.98.6.102192.168.2.78 0497262025483 11/29/22- 16:52:31.441372	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49726	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9732802024313 11/29/22- 16:52:36.325135	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49732	80	192.168.2.7	141.98.6.102

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7141.98.6.1024 9726802024318 11/29/22-16:52:31.339365	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49726	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9728802025381 11/29/22-16:52:32.198993	TCP	2025381	ET TROJAN LokiBot Checkin	49728	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9723802021641 11/29/22-16:52:30.023507	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49723	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9732802024318 11/29/22-16:52:36.325135	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49732	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9720802021641 11/29/22-16:52:28.227779	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49720	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9718802024318 11/29/22-16:52:27.285136	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49718	80	192.168.2.7	141.98.6.102
141.98.6.102192.168.2.78 0497192025483 11/29/22-16:52:27.888790	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49719	141.98.6.102	192.168.2.7
192.168.2.7141.98.6.1024 9729802024318 11/29/22-16:52:32.689634	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49729	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9731802825766 11/29/22-16:52:33.757391	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49731	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9729802024313 11/29/22-16:52:32.689634	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49729	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9730802024318 11/29/22-16:52:33.273429	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49730	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9730802024313 11/29/22-16:52:33.273429	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49730	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9721802025381 11/29/22-16:52:28.704063	TCP	2025381	ET TROJAN LokiBot Checkin	49721	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9724802024318 11/29/22-16:52:30.488585	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49724	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9718802024313 11/29/22-16:52:27.285136	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49718	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9720802825766 11/29/22-16:52:28.227779	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49720	80	192.168.2.7	141.98.6.102
192.168.2.7141.98.6.1024 9724802024313 11/29/22-16:52:30.488585	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49724	80	192.168.2.7	141.98.6.102

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:52:24.997996092 CET	49716	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:25.025604963 CET	80	49716	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:25.025755882 CET	49716	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:25.029133081 CET	49716	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:25.056865931 CET	80	49716	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:25.057019949 CET	49716	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:25.084474087 CET	80	49716	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:25.134174109 CET	80	49716	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:25.134202957 CET	80	49716	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:25.134368896 CET	49716	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:25.134368896 CET	49716	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:25.483601093 CET	49716	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:25.510782003 CET	80	49716	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:25.628839970 CET	49717	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:26.658721924 CET	80	49717	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:26.658849001 CET	49717	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:26.668343067 CET	49717	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:26.696173906 CET	80	49717	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:26.698062897 CET	49717	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:26.725455999 CET	80	49717	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:26.780868053 CET	80	49717	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:26.782255888 CET	49717	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:26.787746906 CET	80	49717	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:26.791439056 CET	49717	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:26.811738968 CET	80	49717	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.252202988 CET	49718	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.279365063 CET	80	49718	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.279613972 CET	49718	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.285135984 CET	49718	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.313250065 CET	80	49718	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.313807011 CET	49718	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.340986967 CET	80	49718	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.393636942 CET	80	49718	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.393665075 CET	80	49718	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.394037962 CET	49718	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.394037962 CET	49718	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.421232939 CET	80	49718	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.755188942 CET	49719	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.782188892 CET	80	49719	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.782548904 CET	49719	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.785438061 CET	49719	80	192.168.2.7	141.98.6.102

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:52:27.812939882 CET	80	49719	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.813057899 CET	49719	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.840610981 CET	80	49719	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.888789892 CET	80	49719	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.888820887 CET	80	49719	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:27.888894081 CET	49719	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.889062881 CET	49719	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:27.916518927 CET	80	49719	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.194387913 CET	49720	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.224909067 CET	80	49720	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.224987030 CET	49720	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.227778912 CET	49720	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.258918047 CET	80	49720	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.259017944 CET	49720	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.287642002 CET	80	49720	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.346106052 CET	80	49720	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.346132994 CET	80	49720	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.346256971 CET	49720	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.346374989 CET	49720	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.374067068 CET	80	49720	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.664561987 CET	49721	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.696398973 CET	80	49721	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.697771072 CET	49721	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.704062939 CET	49721	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.731311083 CET	80	49721	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.731426001 CET	49721	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.758908033 CET	80	49721	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.798693895 CET	80	49721	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.798743010 CET	80	49721	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:28.798816919 CET	49721	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.798846960 CET	49721	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:28.825839996 CET	80	49721	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:29.469907999 CET	49722	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:29.496885061 CET	80	49722	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:29.497585058 CET	49722	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:29.504055977 CET	49722	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:29.531132936 CET	80	49722	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:29.535098076 CET	49722	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:29.563505888 CET	80	49722	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:29.613061905 CET	80	49722	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:29.613097906 CET	80	49722	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:29.613223076 CET	49722	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:29.613276958 CET	49722	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:29.640557051 CET	80	49722	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:29.990570068 CET	49723	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:30.019546986 CET	80	49723	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:30.019854069 CET	49723	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:30.023507118 CET	49723	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:30.051748991 CET	80	49723	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:30.051918030 CET	49723	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:30.080476999 CET	80	49723	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:30.124555111 CET	80	49723	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:30.124568939 CET	80	49723	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:30.124695063 CET	49723	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:30.124789000 CET	49723	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:30.153004885 CET	80	49723	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:30.451586008 CET	49724	80	192.168.2.7	141.98.6.102
Nov 29, 2022 16:52:30.484905958 CET	80	49724	141.98.6.102	192.168.2.7
Nov 29, 2022 16:52:30.485016108 CET	49724	80	192.168.2.7	141.98.6.102

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:51:27.731278896 CET	61178	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:51:27.812835932 CET	63926	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:51:29.055094004 CET	53336	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:51:29.128258944 CET	51007	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:24.965707064 CET	50024	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:24.983006954 CET	53	50024	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:25.609745979 CET	49516	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:25.627433062 CET	53	49516	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:27.231417894 CET	62679	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:27.248811960 CET	53	62679	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:27.735085964 CET	61392	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:27.754470110 CET	53	61392	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:28.174541950 CET	52104	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:28.192017078 CET	53	52104	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:28.646147966 CET	65356	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:28.663779020 CET	53	65356	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:29.136881113 CET	59006	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:29.469077110 CET	53	59006	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:29.972295046 CET	51526	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:29.989815950 CET	53	51526	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:30.432616949 CET	51139	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:30.450237989 CET	53	51139	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:30.865406036 CET	58784	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:30.884907961 CET	53	58784	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:31.290296078 CET	57970	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:31.307420969 CET	53	57970	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:31.765007019 CET	64608	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:31.782563925 CET	53	64608	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:32.148758888 CET	58746	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:32.166456938 CET	53	58746	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:32.638763905 CET	62433	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:32.656164885 CET	53	62433	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:33.218455076 CET	61248	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:33.237142086 CET	53	61248	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:33.705962896 CET	52750	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:33.725223064 CET	53	52750	8.8.8.8	192.168.2.7
Nov 29, 2022 16:52:36.268440008 CET	64078	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:52:36.289087057 CET	53	64078	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:51:27.731278896 CET	192.168.2.7	8.8.8.8	0xba30	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:27.812835932 CET	192.168.2.7	8.8.8.8	0xe1a	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:29.055094004 CET	192.168.2.7	8.8.8.8	0x8f25	Standard query (0)	edi4gw.db.files.1drv.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:51:29.128258944 CET	192.168.2.7	8.8.8.8	0xfe5b	Standard query (0)	edi4gw.db.files.1drv.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:24.965707064 CET	192.168.2.7	8.8.8.8	0xa4c6	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:25.609745979 CET	192.168.2.7	8.8.8.8	0x4b90	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:27.231417894 CET	192.168.2.7	8.8.8.8	0xdf42	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:27.735085964 CET	192.168.2.7	8.8.8.8	0x3e67	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:28.174541950 CET	192.168.2.7	8.8.8.8	0x8a32	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:52:28.646147966 CET	192.168.2.7	8.8.8.8	0xed58	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:29.136881113 CET	192.168.2.7	8.8.8.8	0xe22e	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:29.972295046 CET	192.168.2.7	8.8.8.8	0xd42a	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:30.432616949 CET	192.168.2.7	8.8.8.8	0xaba4	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:30.865406036 CET	192.168.2.7	8.8.8.8	0x843c	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:31.290296078 CET	192.168.2.7	8.8.8.8	0xcea1	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:31.765007019 CET	192.168.2.7	8.8.8.8	0xbf29	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:32.148758888 CET	192.168.2.7	8.8.8.8	0x2cc8	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:32.638763905 CET	192.168.2.7	8.8.8.8	0xf86b	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:33.218455076 CET	192.168.2.7	8.8.8.8	0x904c	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:33.705962896 CET	192.168.2.7	8.8.8.8	0x2ec1	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:36.268440008 CET	192.168.2.7	8.8.8.8	0xc48e	Standard query (0)	sedesadre.gq	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:51:27.775491953 CET	8.8.8.8	192.168.2.7	0xba30	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:27.832566023 CET	8.8.8.8	192.168.2.7	0xe1a	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:29.099885941 CET	8.8.8.8	192.168.2.7	0x8f25	No error (0)	edi4gw.db.files.1drv.com	db-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:29.099885941 CET	8.8.8.8	192.168.2.7	0x8f25	No error (0)	db-files.fe.1drv.com	odc-db-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:29.172468901 CET	8.8.8.8	192.168.2.7	0xfe5b	No error (0)	edi4gw.db.files.1drv.com	db-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:29.172468901 CET	8.8.8.8	192.168.2.7	0xfe5b	No error (0)	db-files.fe.1drv.com	odc-db-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:51:29.172468901 CET	8.8.8.8	192.168.2.7	0xfe5b	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:24.983006954 CET	8.8.8.8	192.168.2.7	0xa4c6	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:25.627433062 CET	8.8.8.8	192.168.2.7	0x4b90	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:27.248811960 CET	8.8.8.8	192.168.2.7	0xdf42	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:27.754470110 CET	8.8.8.8	192.168.2.7	0x3e67	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:28.192017078 CET	8.8.8.8	192.168.2.7	0x8a32	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:28.663779020 CET	8.8.8.8	192.168.2.7	0xed58	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:29.469077110 CET	8.8.8.8	192.168.2.7	0xe22e	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false

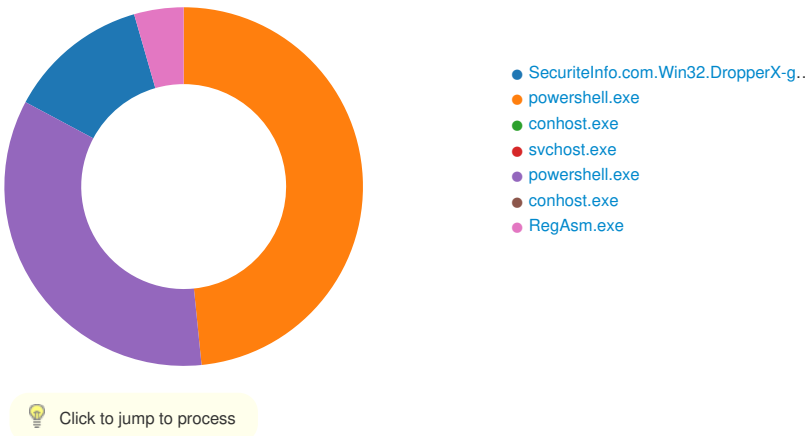
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:52:29.989815950 CET	8.8.8.8	192.168.2.7	0xd42a	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:30.450237989 CET	8.8.8.8	192.168.2.7	0xaba4	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:30.884907961 CET	8.8.8.8	192.168.2.7	0x843c	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:31.307420969 CET	8.8.8.8	192.168.2.7	0xcea1	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:31.782563925 CET	8.8.8.8	192.168.2.7	0xbf29	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:32.166456938 CET	8.8.8.8	192.168.2.7	0x2cc8	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:32.656164885 CET	8.8.8.8	192.168.2.7	0xf86b	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:33.237142086 CET	8.8.8.8	192.168.2.7	0x904c	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:33.725223064 CET	8.8.8.8	192.168.2.7	0x2ec1	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:52:36.289087057 CET	8.8.8.8	192.168.2.7	0xc48e	No error (0)	sedesadre.gq		141.98.6.102	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- sedesadre.gq

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe PID: **5092**, Parent PID: **3320**

General

Target ID:	0
Start time:	16:50:23
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe
Imagebase:	0xd60000
File size:	313856 bytes
MD5 hash:	3039FA7B347872C33C247581A27A7560
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.521369809.0000000003243000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.528024280.00000000042B9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.521045812.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.521045812.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.521045812.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.521045812.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.521045812.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.521045812.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.527878465.0000000004291000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.527878465.0000000004291000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.527878465.0000000004291000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.527878465.0000000004291000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.527878465.0000000004291000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.527878465.0000000004291000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D7CCF06	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	6D7CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DADC78D	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\SecuriteInfo.com.Win32.DropperX-gen.15139.3101.exe.log	0	1537	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",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",02,"System.Windows.Forms, Vers	success or wait	1	6DADC907	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	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7003DE	ReadFile
\pipe	unknown	1024	success or wait	1	6C611B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D7003DE	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **1508**, Parent PID: **5092**

General

Target ID:	1
Start time:	16:50:23
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"powershell" Get-Date
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kk3bso0d.u4o.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C611E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_150mte30.zn5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C611E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C611E60	CreateFileW
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	6D7CCF06	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	6D7CCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kk3bso0d.u4o.ps1	success or wait	1	6C616A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_150mte30.zn5.psm1	success or wait	1	6C616A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kk3bso0d.u4o.ps1	0	1	31	1	success or wait	1	6C611B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_150mte30.zn5.psm1	0	1	31	1	success or wait	1	6C611B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C611B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	6C611B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 1d 0e 00 00 12 00 00 00 fd 0e 20 06 fd 08 fd 08 fd 07 00 00 00 01 27 00 13 00 fd 0e 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e '@	success or wait	1	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6DA976FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	9	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 16 3b 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M?M;@BMDmE;@;@<@<@EMqqS	success or wait	9	6DA976FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D7B1F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7003DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C611B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C611B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C611B4F	ReadFile

Analysis Process: conhost.exe PID: **5700**, Parent PID: **1508**

General

Target ID:	2
Start time:	16:50:24
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **2084**, Parent PID: **552**

General

Target ID:	5
Start time:	16:50:41
Start date:	29/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff732630000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **1376**, Parent PID: **5092**

General

Target ID:	12
Start time:	16:51:46
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hojog3ew.0sb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C611E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cdh4roqr.3j3.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C611E60	CreateFileW

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	6D7CCF06	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	6D7CCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hojog3ew.0sb.ps1	success or wait	1	6C616A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cdh4roqr.3j3.psm1	success or wait	1	6C616A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	257	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	276	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	297	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	313	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	321	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	330	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
unknown	338	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C575B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hojog3ew.0sb.ps1	0	1	31	1	success or wait	1	6C611B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cdh4roqr.3j3.psm1	0	1	31	1	success or wait	1	6C611B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 1d 0e 00 00 12 00 00 00 fd 0e 20 06 fd 08 fd 08 fd 07 00 00 00 01 27 00 13 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@e '@	success or wait	1	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6DA976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6DA976FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 16 3b 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M?M;@BMDmE;@;@<@<@EMqqS	success or wait	8	6DA976FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7003DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D7B1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	18184	success or wait	1	6D7B203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7003DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	6C611B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C611B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C611B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C611B4F	ReadFile

Analysis Process: conhost.exe PID: **5096**, Parent PID: **1376**

General

Target ID:	13
Start time:	16:51:46
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: **2084**, Parent PID: **5092**

General

Target ID:	14
Start time:	16:52:22
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x650000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 0000000E.00000000.513382566.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.513552356.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 0000000E.00000000.513552356.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 0000000E.00000000.513552356.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 0000000E.00000000.513552356.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

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

File Deleted

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

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

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

File Read

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

Disassembly

No disassembly