ID: 433227
Sample Name:
SecuriteInfo.com.Variant.MSILHeracles.17940.23513.15553
Cookbook: default.jbs
Time: 13:54:21
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

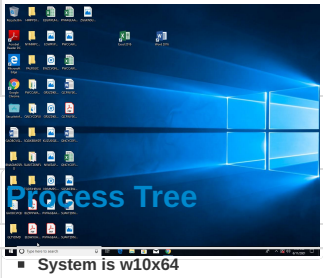
Analysis Report SecuriteInfo.com.Variant.MSILHeracles…

Overview

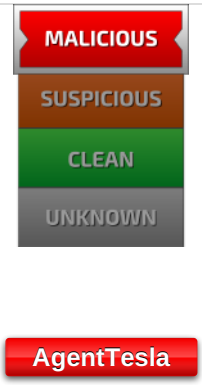
General Information

Sample Name:	SecuriteInfo.com.Variant.MSILHeracles.17940.23513.15553 (renamed file extension from 15553 to exe)
Analysis ID:	433227
MD5:	95201005885c91..
SHA1:	d172e70ecb7f320.
SHA256:	73f2e9b534cff49…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

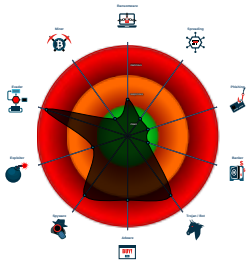


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Modifies the hosts file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



- **System is w10x64**
- SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe (PID: 6136 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe' MD5: 95201005885C91DB292ADAAE627A5D57)
  - RegSvcs.exe (PID: 5636 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- NXLun.exe (PID: 4712 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NXLun.exe (PID: 4128 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "operations@priserveinfra.comoppipl121019mail.priserveinfra.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.201228524.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.201228524.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.460330476.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.460330476.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.203209096.000000000439 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Variant.MSILHeracles.17940.23 513.exe.44b9398.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected AgentTesla

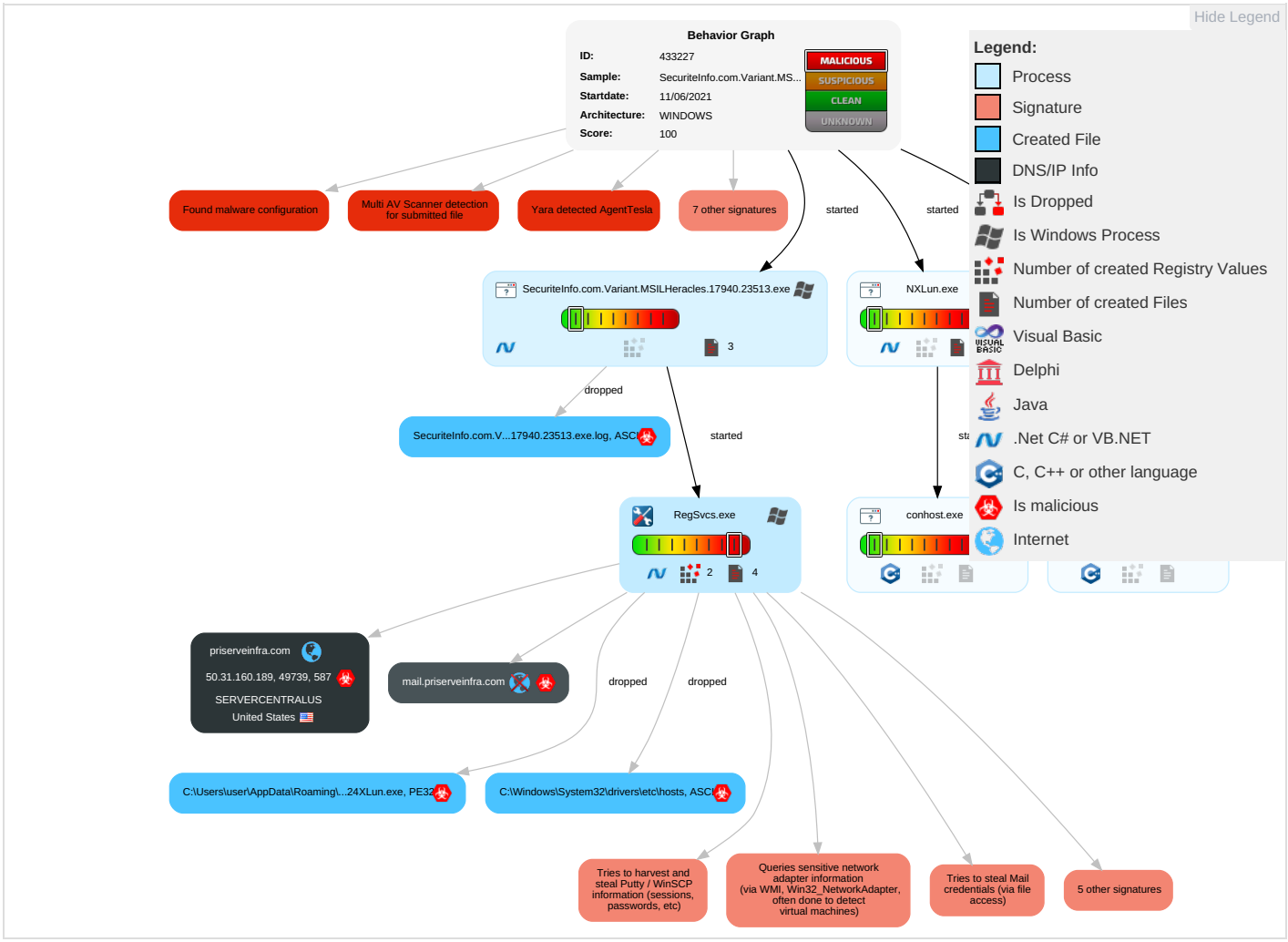
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

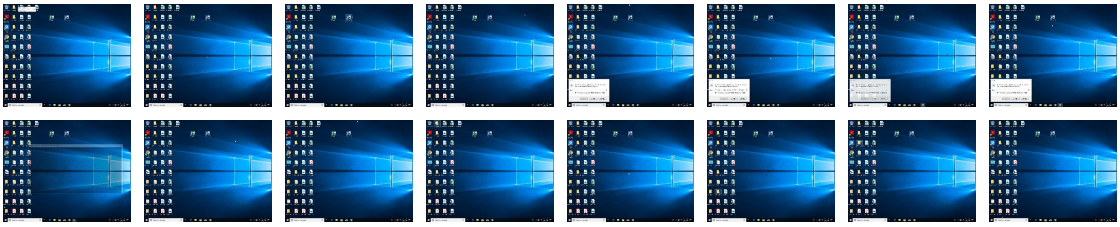
Behavior Graph



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.Variant.MSILHeracles.17940.23513.exe	32%	Virustotal		Browse
SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	0%	ReversingLabs		

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
priserveinfra.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/01	0%	Virustotal		Browse
http://r3.i.lencr.org/01	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://CvqG2KRIY7VhTa.o	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://CvqG2KRIY7VhTa.org	0%	Avira URL Cloud	safe	
http://hcwBaC.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.priserveinfra.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://priserveinfra.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
priserveinfra.com	50.31.160.189	true	true	• 1%, Virustotal, Browse	unknown
mail.priserveinfra.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.31.160.189	priserveinfra.com	United States		23352	SERVERCENTRALUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433227
Start date:	11.06.2021
Start time:	13:54:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.MSILHeracles.17940.23513.15553 (renamed file extension from 15553 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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.adwa.spyw.evad.winEXE@7/6@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.5%) • Quality average: 48.6% • Quality standard deviation: 46%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:55:07	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe modified
13:55:16	API Interceptor	766x Sleep call for process: RegSvcs.exe modified
13:55:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NXLun C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
13:55:36	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run NXLun C:\Users\user\AppData\Roaming\NXLun\NXLun.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.31.160.189	SecuriteInfo.com.Exploit.Siggen2.12917.8592.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Siggen2.12943.15385.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	Doc-20200731-7729500.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	doc_440.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	MES 2020_07_31 9325071.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	arc GNV011047.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	ARC_4895987.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	Rep-OVW91546.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	REP_OKX598.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	FILE-2020_07_31-LY51195.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	REP-2020_07_31-HL73628.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/
	Dat_20200731_ILT3900.doc	Get hash	malicious	Browse	• jkncrew.com/cgi-bin/KhSO16ZAAf/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVERCENTRALUS	619wGDCTZA.exe	Get hash	malicious	Browse	• 216.246.112.102
	Swift Copy.exe	Get hash	malicious	Browse	• 204.93.196.181
	Swift Copy.exe	Get hash	malicious	Browse	• 204.93.196.181
	Swift Copy.exe	Get hash	malicious	Browse	• 204.93.196.181
	PO #4500484210.exe	Get hash	malicious	Browse	• 204.93.196.181
	Quotation 2000051165.exe	Get hash	malicious	Browse	• 204.93.196.181
	RYJzamn1HwAEPyy.exe	Get hash	malicious	Browse	• 50.31.160.189
	Swift Copy.exe	Get hash	malicious	Browse	• 204.93.196.181
	Revised_Order PDF.exe	Get hash	malicious	Browse	• 198.38.93.60
	tB15iC3ImLK3MFX.exe	Get hash	malicious	Browse	• 50.31.160.189
	Bank Details.exe	Get hash	malicious	Browse	• 204.93.196.181
	Bank Details.exe	Get hash	malicious	Browse	• 204.93.196.181
	tYIAJnu9nz5cOsZ.exe	Get hash	malicious	Browse	• 50.31.160.189
	Bank Details.exe	Get hash	malicious	Browse	• 204.93.196.181
	Bank Details.exe	Get hash	malicious	Browse	• 204.93.196.181
	upnxIVxCnyXyWyW.exe	Get hash	malicious	Browse	• 50.31.160.189
	1092991(JB#082).exe	Get hash	malicious	Browse	• 204.93.196.181
	1092991(JB#082).exe	Get hash	malicious	Browse	• 204.93.196.181
	uDEF0FNW0uvax8f.exe	Get hash	malicious	Browse	• 204.93.196.181
	payment.exe	Get hash	malicious	Browse	• 204.93.196.181

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	HT210525 IV Quotation.exe	Get hash	malicious	Browse	
	Bank_payment information.exe	Get hash	malicious	Browse	
	HT210525 IV Quotation.exe	Get hash	malicious	Browse	
	Proforma Invoice No. 14214.exe	Get hash	malicious	Browse	
	KCTC International Ltd.exe	Get hash	malicious	Browse	
	NEW PO#70-02110-00739.exe	Get hash	malicious	Browse	
	New quote.exe	Get hash	malicious	Browse	
	Bank payment information.exe	Get hash	malicious	Browse	
	MESCO TQZ24 QUOTE.exe	Get hash	malicious	Browse	
	SWIFT Msg of USD 78,000.exe	Get hash	malicious	Browse	
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	
	ORDER #2348478.exe	Get hash	malicious	Browse	
	1029BA046DF67EE328AD9D21BFD1E6D31C5CEDC4D4EAD.exe	Get hash	malicious	Browse	
	Quotation 2000051165.exe	Get hash	malicious	Browse	
	IMG-20191224-WA0050.jpg.exe	Get hash	malicious	Browse	
	Note0093746573.exe	Get hash	malicious	Browse	
	RYJzamn1HwAEPyy.exe	Get hash	malicious	Browse	
	11.exe	Get hash	malicious	Browse	
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	
	NEW Quotation.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NXLun.exe.log	
Process:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: HT210525 IV Quotation.exe, Detection: malicious, Browse • Filename: Bank_payment information.exe, Detection: malicious, Browse • Filename: HT210525 IV Quotation.exe, Detection: malicious, Browse • Filename: Proforma Invoice No. 14214.exe, Detection: malicious, Browse • Filename: KCTC International Ltd.exe, Detection: malicious, Browse • Filename: NEW PO#70-02110-00739.exe, Detection: malicious, Browse • Filename: New quote.exe, Detection: malicious, Browse • Filename: Bank payment information.exe, Detection: malicious, Browse • Filename: MESCO TQZ24 QUOTE.exe, Detection: malicious, Browse • Filename: SWIFT Msg of USD 78,000.exe, Detection: malicious, Browse • Filename: OM PHOENIX TRADERS.exe, Detection: malicious, Browse • Filename: ORDER #2348478.exe, Detection: malicious, Browse • Filename: 1029BA046DF67EE328AD9D21BFD1E6D31C5CEDC4D4EAD.exe, Detection: malicious, Browse • Filename: Quotation 2000051165.exe, Detection: malicious, Browse • Filename: IMG-20191224-WA0050.jpg.exe, Detection: malicious, Browse • Filename: Note0093746573.exe, Detection: malicious, Browse • Filename: RYJzamn1HwAEPyy.exe, Detection: malicious, Browse • Filename: 11.exe, Detection: malicious, Browse • Filename: OM PHOENIX TRADERS.exe, Detection: malicious, Browse • Filename: NEW Quotation.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141

\Device\ConDrv	
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.493580728299334
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe
File size:	930816
MD5:	95201005885c91db292adaae627a5d57
SHA1:	d172e70ecb7f3206bcd34d7d5b51be54d9bdc350
SHA256:	73f2e9b534cff49f248d0d3469902ac7c3150da888786e5cde16a935ce4ce0c2
SHA512:	b571adb6cd73909e7d93311401dd8c96168cae2fba009e063786b7bc87a56e0d1d361ac0b76f2531458c315e354b981b8725fd67f9b33ed5b98fa7cb6a368ca7
SSDEEP:	12288:4IiPCg6zYjxAYcfPxu87cSumg7G+pPM0rgpmDKuedZM4e/ZUdtb:4NPC1zSeHXh7cH66PmwDxedNeBUdt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....>.... .....@.. .....@.....

File Icon

Icon Hash:	8c8caa8e9692aa00

Static PE Info

General

Entrypoint:	0x4ba63e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C2AE0F [Fri Jun 11 00:27:59 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4

General

Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb8644	0xb8800	False	0.892889090024	data	7.85141834625	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xbc000	0x1e8	0x200	False	0.861328125	data	6.62043448152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x2a388	0x2a400	False	0.124312361317	data	4.17146470655	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 13:56:40.678406954 CEST	192.168.2.3	8.8.8.8	0xce81	Standard query (0)	mail.priserveinfra.com	A (IP address)	IN (0x0001)
Jun 11, 2021 13:56:40.860426903 CEST	192.168.2.3	8.8.8.8	0x8b1e	Standard query (0)	mail.priserveinfra.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 13:56:40.850236893 CEST	8.8.8.8	192.168.2.3	0xce81	No error (0)	mail.priserveinfra.com	priserveinfra.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:56:40.850236893 CEST	8.8.8.8	192.168.2.3	0xce81	No error (0)	priserveinfra.com		50.31.160.189	A (IP address)	IN (0x0001)
Jun 11, 2021 13:56:41.040086985 CEST	8.8.8.8	192.168.2.3	0x8b1e	No error (0)	mail.priserveinfra.com	priserveinfra.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:56:41.040086985 CEST	8.8.8.8	192.168.2.3	0x8b1e	No error (0)	priserveinfra.com		50.31.160.189	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 13:56:41.598962069 CEST	587	49739	50.31.160.189	192.168.2.3	220-metro702.hostmetro.com ESMTP Exim 4.94.2 #2 Fri, 11 Jun 2021 06:56:41 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 13:56:41.599651098 CEST	49739	587	192.168.2.3	50.31.160.189	EHLO 936905
Jun 11, 2021 13:56:41.743532896 CEST	587	49739	50.31.160.189	192.168.2.3	250-metro702.hostmetro.com Hello 936905 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 11, 2021 13:56:41.744143963 CEST	49739	587	192.168.2.3	50.31.160.189	STARTTLS
Jun 11, 2021 13:56:41.909204960 CEST	587	49739	50.31.160.189	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe PID: 6136 Parent PID: 5820

General

Start time:	13:55:06
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe'
Imagebase:	0xe40000
File size:	930816 bytes
MD5 hash:	95201005885C91DB292ADAAE627A5D57
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.203209096.0000000004399000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.203209096.0000000004399000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.202906740.00000000033C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 5636 Parent PID: 6136

General

Start time:	13:55:08
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xf10000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.201228524.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.201228524.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.460330476.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.460330476.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.462879077.0000000003171000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.462879077.0000000003171000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: NXLun.exe PID: 4712 Parent PID: 3388

General

Start time:	13:55:36
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe'
Imagebase:	0x420000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4732 Parent PID: 4712

General

Start time:	13:55:36
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: NXLun.exe PID: 4128 Parent PID: 3388

General

Start time:	13:55:44
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe'
Imagebase:	0x540000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 4140 Parent PID: 4128

General

Start time:	13:55:44
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis