ID: 458957
Sample Name: PI A19T010620.exe
Cookbook: default.jbs
Time: 22:48:18
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

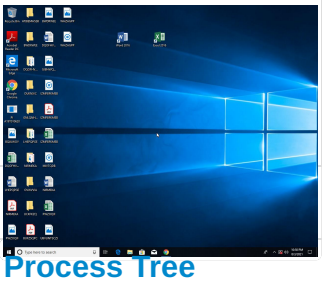
Windows Analysis Report PI A19T010620.exe

Overview

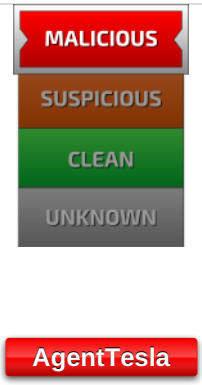
General Information

Sample Name:	PI A19T010620.exe
Analysis ID:	458957
MD5:	62aaab0942211b..
SHA1:	2703f7f409aeb01..
SHA256:	23e9628689de5c..
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection



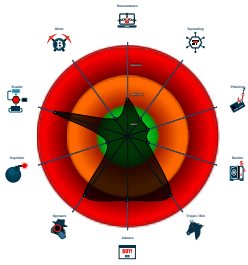
AgentTesla

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
- .NET source code contains very larg…
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Modifies the hosts file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- PI A19T010620.exe (PID: 7024 cmdline: 'C:\Users\user\Desktop\PI A19T010620.exe' MD5: 62AAAB0942211B9D11A7755D1970ADFD)
  - RegSvcs.exe (PID: 6464 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- NXLun.exe (PID: 7164 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NXLun.exe (PID: 2432 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 7084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "compliance2@odessabd.com",
  "Password": "abc321",
  "Host": "mail.odessabd.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.899781379.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.899781379.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.901158157.000000000241000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegSvcs.exe PID: 6464	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: RegSvcs.exe PID: 6464	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

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	

Sigma Overview

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Jbx 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

.NET source code contains very large strings

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Modifies the hosts file

Writes to foreign memory regions

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:

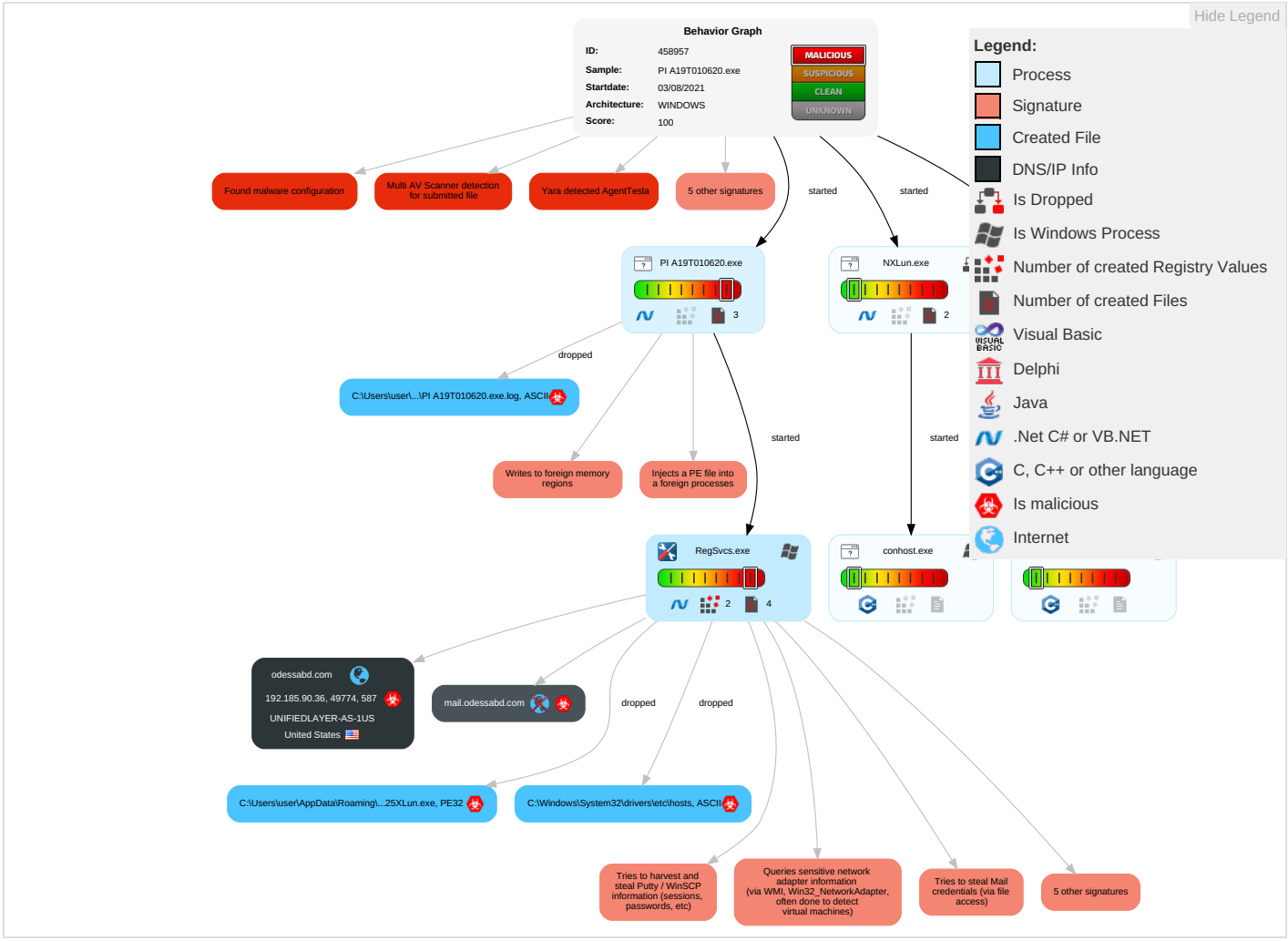
Yara detected AgentTesla

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 2 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	Credentials in Registry 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 1 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatior
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	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 Communicatic
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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
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 Protocol

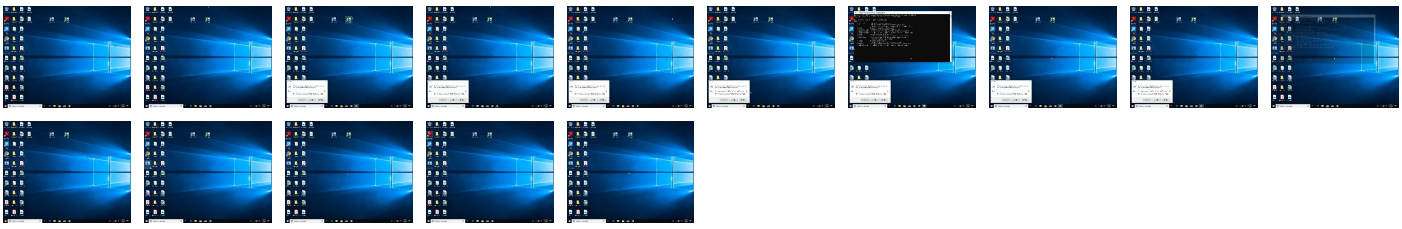
Behavior Graph



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
PI A19T010620.exe	51%	Virustotal		Browse
PI A19T010620.exe	51%	Metadefender		Browse
PI A19T010620.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PI A19T010620.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

Domains

Source	Detection	Scanner	Label	Link
odessabd.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
mail.odessabd.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	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://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://crl.microsoft.co9	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://mOEDeY.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://cps.letsencrypt.o_	0%	Avira URL Cloud	safe	
http://mail.odessabd.com	0%	Avira URL Cloud	safe	
http://P02rvktl5O.com	0%	Avira URL Cloud	safe	
http://odessabd.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://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://https://static.hummingbird.me/anime/poster_images/000/010/716/large/0fd8df1b586e60a0b1591cd8555c072f	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
odessabd.com	192.185.90.36	true	true	• 0%, Virustotal, Browse	unknown
mail.odessabd.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.90.36	odessabd.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458957
Start date:	03.08.2021
Start time:	22:48:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI A19T010620.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:	18
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:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:49:19	API Interceptor	1x Sleep call for process: PI A19T010620.exe modified
22:49:31	API Interceptor	665x Sleep call for process: RegSvcs.exe modified
22:49:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NXLun C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
22:49:50	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
192.185.90.36	PO-K-128 IAN 340854.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Payment_Advice.exe	Get hash	malicious	Browse	• 173.254.28.149
	RuVwYj2Jax.exe	Get hash	malicious	Browse	• 192.185.77.139
	KkPVouLuOx.exe	Get hash	malicious	Browse	• 67.20.76.71
	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 162.241.218.97
	wuxvGLNrxG.jar	Get hash	malicious	Browse	• 162.241.216.53
	Amaury.vanvinckenroye-AudioMessage_520498.htm	Get hash	malicious	Browse	• 192.185.138.88
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 50.87.146.49
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 74.220.199.6
	hD72Gd3THG.exe	Get hash	malicious	Browse	• 67.20.76.71
	Products Order38899999.exe	Get hash	malicious	Browse	• 50.87.146.199
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 74.220.199.6
	WWTLJo3vxn.exe	Get hash	malicious	Browse	• 192.254.235.241
	INV. 736392 Scan pdf.exe	Get hash	malicious	Browse	• 192.185.164.148
	7nNtjBvhrm	Get hash	malicious	Browse	• 142.7.147.90
	Purchase Requirements.exe	Get hash	malicious	Browse	• 192.185.0.218
	#Ud83d#Udda8 FaxMail dir -INV 000087.html	Get hash	malicious	Browse	• 162.241.217.69
	Products Order.exe	Get hash	malicious	Browse	• 50.87.146.199
	zerYOlEkZR.exe	Get hash	malicious	Browse	• 192.254.235.241
	PO-K-128 IAN 340854.exe	Get hash	malicious	Browse	• 192.185.90.36
	csa customers.xlsx	Get hash	malicious	Browse	• 162.241.217.138

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	Swift Copy.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	POSH service quotation.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	epda.exe	Get hash	malicious	Browse	
	POSH service quotation..exe	Get hash	malicious	Browse	
	SWIFT REF GO 20210730SFT21020137.exe	Get hash	malicious	Browse	
	HJKcEjrUuzYMV9X.exe	Get hash	malicious	Browse	
	est pda.exe	Get hash	malicious	Browse	
	BL COPY.exe	Get hash	malicious	Browse	
	DOC.exe	Get hash	malicious	Browse	
	statement.exe	Get hash	malicious	Browse	
	PO-K-128 IAN 340854.exe	Get hash	malicious	Browse	
	PO#4500484210.exe	Get hash	malicious	Browse	
	Invoice no SS21-22185.exe	Get hash	malicious	Browse	
	SQycD6hL4Y.exe	Get hash	malicious	Browse	
	Aggiornamento ordine Quantit#U00e0__BFM Srl 117-28050-01.exe	Get hash	malicious	Browse	
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	
	FINAL SHIPPING DOC..exe	Get hash	malicious	Browse	
	Spare Parts Requisition-003,004.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NXLun.exe.log	
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\PI A19T010620.exe.log	
Process:	C:\Users\user\Desktop\PI A19T010620.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:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4DB42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	
Joe Sandbox View:	• Filename: Swift Copy.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: POSH service quotation.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: epda.exe, Detection: malicious, Browse • Filename: POSH service quotation..exe, Detection: malicious, Browse • Filename: SWIFT REF GO 20210730SFT21020137.exe, Detection: malicious, Browse • Filename: HJKcEjrUuzYMV9X.exe, Detection: malicious, Browse • Filename: est pda.exe, Detection: malicious, Browse • Filename: BL COPY.exe, Detection: malicious, Browse • Filename: DOC.exe, Detection: malicious, Browse • Filename: statement.exe, Detection: malicious, Browse • Filename: PO-K-128 IAN 340854.exe, Detection: malicious, Browse • Filename: PO#4500484210.exe, Detection: malicious, Browse • Filename: Invoice no SS21-22185.exe, Detection: malicious, Browse • Filename: SQycD6hL4Y.exe, Detection: malicious, Browse • Filename: Aggiornamento ordine Quantit#U00e0__BFM Srl 117-28050-01.exe, Detection: malicious, Browse • Filename: PAYMENT INSTRUCTIONS COPY.exe, Detection: malicious, Browse • Filename: FINAL SHIPPING DOC..exe, Detection: malicious, Browse • Filename: Spare Parts Requisition-003,004.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**
Reputation:	high, very likely benign file
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
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

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.916784541748945
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PI A19T010620.exe
File size:	1141760
MD5:	62aaab0942211b9d11a7755d1970adfd
SHA1:	2703f7f409aeb01b0d68e83f336241f4b7923532
SHA256:	23e9628689de5cffc14abcc1d39a259f54bde8e50304af29d4e127359163e1c4
SHA512:	c408ae66a98fa70b14f2e3527078bd7b1bca862b7f071efdf78caa7fb8b7d82c6de78a088981bda1d48f30034063488fe8094f3e39aedeecdb194755667f13a9
SSDEEP:	24576:YP9ZVh8b4lyJE84wq/dExJaK6ptDPgfqNE5D6+fVahiLXXFM:cNgJaK6LI5+8VFLXV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....b..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5180de
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:	0x6101FAD1 [Thu Jul 29 00:48:17 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1160e4	0x116200	False	0.619296875	data	6.92181951931	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x11a000	0x5fc	0x600	False	0.435546875	data	4.20979745482	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x11c000	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
Aug 3, 2021 22:50:58.386392117 CEST	192.168.2.4	8.8.8.8	0x5dfa	Standard query (0)	mail.odessabd.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:50:58.574436903 CEST	192.168.2.4	8.8.8.8	0xfa23	Standard query (0)	mail.odessabd.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:50:58.556462049 CEST	8.8.8.8	192.168.2.4	0x5dfa	No error (0)	mail.odessabd.com	odessabd.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:50:58.556462049 CEST	8.8.8.8	192.168.2.4	0x5dfa	No error (0)	odessabd.com		192.185.90.36	A (IP address)	IN (0x0001)
Aug 3, 2021 22:50:58.609914064 CEST	8.8.8.8	192.168.2.4	0xfa23	No error (0)	mail.odessabd.com	odessabd.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:50:58.609914064 CEST	8.8.8.8	192.168.2.4	0xfa23	No error (0)	odessabd.com		192.185.90.36	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 22:50:59.108015060 CEST	587	49774	192.185.90.36	192.168.2.4	220-lasalle.websitewelcome.com ESMTP Exim 4.94.2 #2 Tue, 03 Aug 2021 15:50:59 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 3, 2021 22:50:59.108342886 CEST	49774	587	192.168.2.4	192.185.90.36	EHLO 932923
Aug 3, 2021 22:50:59.243237972 CEST	587	49774	192.185.90.36	192.168.2.4	250-lasalle.websitewelcome.com Hello 932923 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 3, 2021 22:50:59.243637085 CEST	49774	587	192.168.2.4	192.185.90.36	STARTTLS
Aug 3, 2021 22:50:59.384365082 CEST	587	49774	192.185.90.36	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PI A19T010620.exe PID: 7024 Parent PID: 5916

General

Start time:	22:49:00
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\PI A19T010620.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI A19T010620.exe'
Imagebase:	0xff0000
File size:	1141760 bytes
MD5 hash:	62AAAB0942211B9D11A7755D1970ADFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 6464 Parent PID: 7024

General

Start time:	22:49:19
Start date:	03/08/2021
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:	0x30000
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: 00000002.00000002.899781379.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.899781379.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.901158157.0000000002401000.00000004.00000001.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: 7164 Parent PID: 3424

General

Start time:	22:49:50
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe'
Imagebase:	0x1b0000
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: 6160 Parent PID: 7164

General

Start time:	22:49:51
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000

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: 2432 Parent PID: 3424

General

Start time:	22:49:58
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe'
Imagebase:	0xab0000
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: 7084 Parent PID: 2432

General

Start time:	22:49:59
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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