

JOeSandbox Cloud BASIC



ID: 458867

Sample Name: POSH service
quotation.exe

Cookbook: default.jbs

Time: 20:17:16

Date: 03/08/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report POSH service quotation.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Jbx Signature Overview	5
AV Detection:	5
Spam, unwanted Advertisements and Ransom Demands:	5
System Summary:	5
Hooking and other Techniques for Hiding and Protection:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	5
Lowering of HIPS / PFW / Operating System Security Settings:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	9
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	13
General	13
File Icon	13
Static PE Info	14
General	14
Entrypoint Preview	14
Data Directories	14
Sections	14
Resources	14
Imports	14
Version Infos	14
Network Behavior	14
Network Port Distribution	14
TCP Packets	14
UDP Packets	14
DNS Queries	14
DNS Answers	15
SMTP Packets	15
Code Manipulations	15
Statistics	15
Behavior	15
System Behavior	15
Analysis Process: POSH service quotation.exe PID: 6888 Parent PID: 5784	15

General	15
File Activities	16
File Created	16
File Written	16
File Read	16
Analysis Process: RegSvc.exe PID: 7096 Parent PID: 6888	16
General	16
File Activities	16
File Created	16
File Written	16
File Read	16
Registry Activities	16
Key Value Created	16
Analysis Process: NXLun.exe PID: 6640 Parent PID: 3424	16
General	16
File Activities	17
File Created	17
File Written	17
File Read	17
Analysis Process: conhost.exe PID: 6692 Parent PID: 6640	17
General	17
Analysis Process: NXLun.exe PID: 5872 Parent PID: 3424	17
General	17
File Activities	17
File Written	18
File Read	18
Analysis Process: conhost.exe PID: 6120 Parent PID: 5872	18
General	18
Disassembly	18
Code Analysis	18

Windows Analysis Report POSH service quotation.exe

Overview

General Information

Sample Name:

POSH service quotation.exe

Analysis ID:

458867

MD5:

fbe4c77e66f8d27..

SHA1:

6d3c4a210029e5..

SHA256:

eb05092bdbc35f2.

Tags:

exe

null

Infos:

Most interesting Screenshot:

Process Tree

- System is w10x64
- POSH service quotation.exe (PID: 6888 cmdline: 'C:\Users\user\Desktop\POSH service quotation.exe' MD5: FBE4C77E66F8D27264B57E4358648DE2)
 - RegSvc.exe (PID: 7096 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvc.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- NXLun.exe (PID: 6640 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
 - conhost.exe (PID: 6692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NXLun.exe (PID: 5872 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
 - conhost.exe (PID: 6120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{  "Exfil Mode": "SMTP",  "Username": "chefcomptable@ndn.edu.lb",  "Password": "Lebanon-Achrafteh-39",  "Host": "mail.ndn.edu.lb"}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.908110927.00000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.908110927.00000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.909617305.0000000002361000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.909617305.0000000002361000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: RegSvcs.exe PID: 7096	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 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	

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

Initial sample is a PE file and has a suspicious name

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:



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:



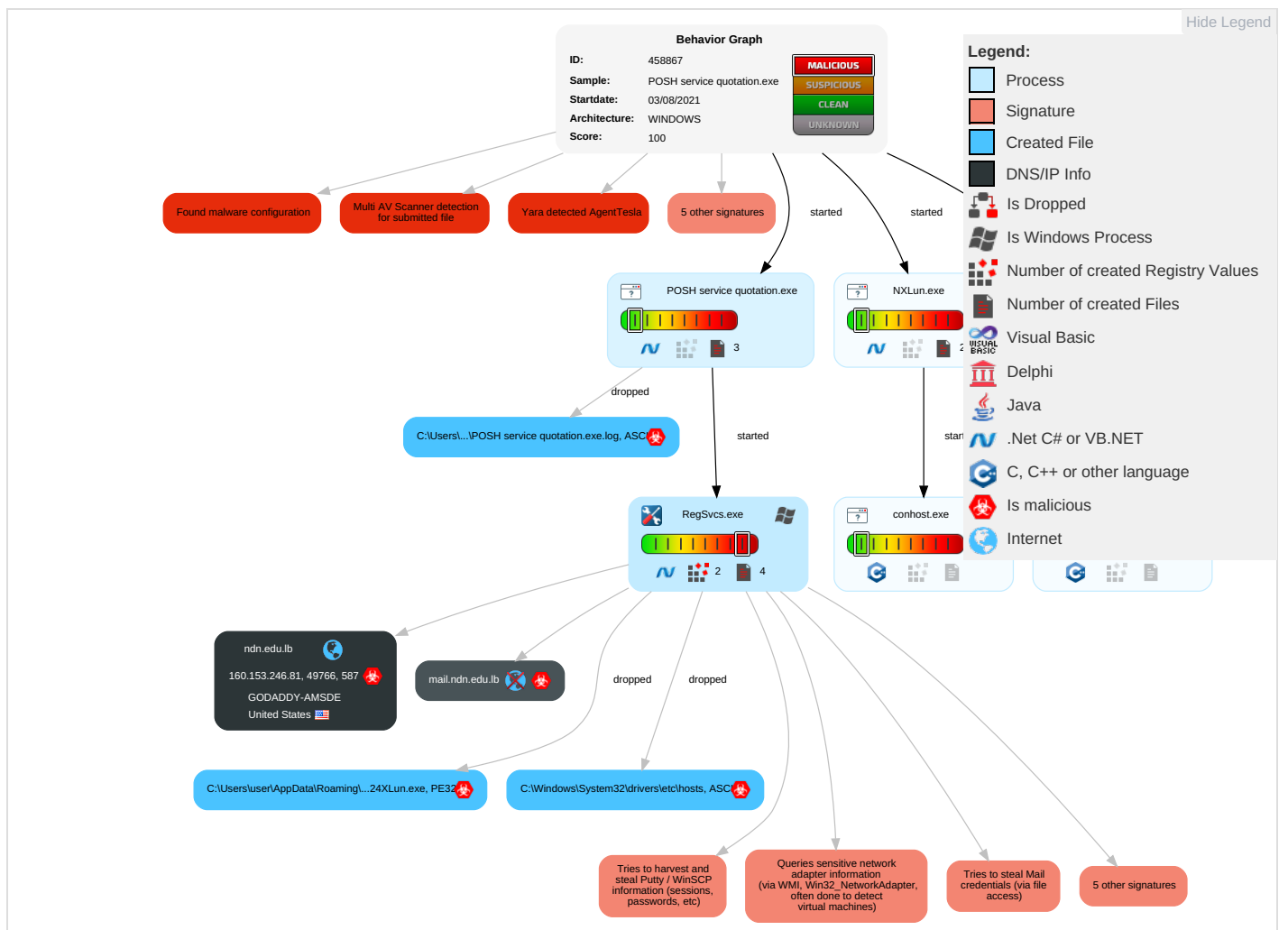
Yara detected AgentTesla

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
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	Normal Port
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	Normal Application Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol
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	Fall Back Channel
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestamp 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiple Correlation
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Correlation Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 3 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Well-Known
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Protocol

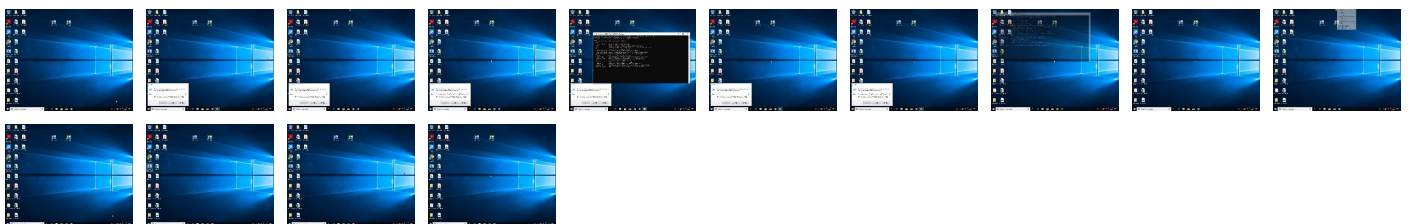
Behavior Graph



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
POSH service quotation.exe	62%	Virustotal		Browse
POSH service quotation.exe	49%	Metadefender		Browse
POSH service quotation.exe	85%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
POSH service quotation.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
ndn.edu.lb	0%	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://https://n7NI8RiXhvBEJFUh.com	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ndn.edu.lb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnM	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnW	0%	Avira URL Cloud	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://www.founder.com.cn/cns	0%	URL Reputation	safe	
http://LFVvwW.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comeB	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://mail.ndn.edu.lb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn=	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.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://www.founder.com.cn/cnYZ	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%\$	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ndn.edu.lb	160.153.246.81	true	true	• 0%, Virustotal, Browse	unknown
mail.ndn.edu.lb	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
160.153.246.81	ndn.edu.lb	United States		21501	GODADDY-AMSDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458867
Start date:	03.08.2021
Start time:	20:17:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	POSH service quotation.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:	20
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: 99% • 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
20:18:22	API Interceptor	1x Sleep call for process: POSH service quotation.exe modified
20:18:31	API Interceptor	687x Sleep call for process: RegSvcs.exe modified
20:18:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NXLun C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
20:18:52	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
160.153.246.81	statement.exe	Get hash	malicious	Browse	
	Invoice no SS21-22185.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	Order - HOM-OS-20-21-5-12.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
GODADDY-AMSDE	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 160.153.138.219
	New_1007572_021.xltx	Get hash	malicious	Browse	• 160.153.129.234
	ORIGINAL PROFORMA INVOICE COAU722089813 0,PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	Purchase Requirements.exe	Get hash	malicious	Browse	• 160.153.136.3
	New order.xltx	Get hash	malicious	Browse	• 160.153.129.234

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	statement.exe	Get hash	malicious	Browse	160.153.246.81
	Purchase Requirements.exe	Get hash	malicious	Browse	160.153.136.3
	Invoice no SS21-22185.exe	Get hash	malicious	Browse	160.153.246.81
	i9Na8iof4G.exe	Get hash	malicious	Browse	160.153.136.3
	2129-20 30% CLAIM - PO SPO21-01-072.exe	Get hash	malicious	Browse	160.153.16.6
	AMxAyl1FvN.doc	Get hash	malicious	Browse	160.153.208.149
	M7ZGK4fBfl.exe	Get hash	malicious	Browse	160.153.136.3
	altnp3zl5hfg3Eg.exe	Get hash	malicious	Browse	160.153.136.3
	gqdJ6f9axq.exe	Get hash	malicious	Browse	160.153.136.3
	YaRh8PG41y.exe	Get hash	malicious	Browse	160.153.136.3
	2129-20 30% CLAIM - PO SPO21-01-072.exe	Get hash	malicious	Browse	160.153.16.6
	Invoice #210722 14,890 \$.exe	Get hash	malicious	Browse	160.153.136.3
	SCAN_Wells Fargo bank payment.exe	Get hash	malicious	Browse	160.153.133.86
	PO.exe	Get hash	malicious	Browse	160.153.246.81
	4bTTNoUZaa.exe	Get hash	malicious	Browse	160.153.136.3

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	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	
	PO NOAB1088 ALEMO INDUSTRIAL ENGINEERS.exe	Get hash	malicious	Browse	
	Order List.exe	Get hash	malicious	Browse	
	PAYMENT BANK INSTRUCTIONS COPY.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NXLun.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f711d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POSH service quotation.exe.log	
Process:	C:\Users\user\Desktop\POSH service quotation.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKKHoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKHqNoPtHoxHhAHY
MD5:	69206D3AF76DEFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	true
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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\System4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\fd8480152e0da9a60ad49c6d16a3b6d\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\Local\Roaming\INXLun\INXLun.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+SdlBf0k2dsYyV6lq87PiU9FVlaLmf:EoOIBf0ddsYy8LujVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D1B42
Malicious:	true
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	- 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 - Filename: PO NOAB1088 ALEMO INDUSTRIAL ENGINEERS.exe, Detection: malicious, Browse - Filename: Order List.exe, Detection: malicious, Browse - Filename: PAYMENT BANK INSTRUCTIONS COPY.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..lc.....d.....`rsrc...8.....f.....@..@..reloc..... ...p.....@..B.....8.....H.....+...S.....P.....r...p(....*2.(....(*z...r.p(....(....)*...*S.....*0.{.....Q..-S.....+i~...0.(.... S.....o...r!..p.(...Q.P.;P.....(....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	

C:\Windows\System32\drivers\etc\hosts	
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

I:\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:zKLXkb4DObntKlgIUEnfQtvNuNpKOK5aM9YJC: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 Suppress 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):	7.146711496574452
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:	POSH service quotation.exe
File size:	1005568
MD5:	fbe4c77e66f8d27264b57e4358648de2
SHA1:	6d3c4a210029e584bca436427d58930a2fc50123
SHA256:	eb05092bdbc35f254d4a38fca26197482f2d81bf6ffb246f4dc7a4a5e4e250f4
SHA512:	5e5cecbdf73e6950b7c0b8984e181f85383bfee22375b9876bdd7f42f362d90c050e022de5fea420a7f63d02a3729f8376da0394e11d48ec695117ff7218016c
SSDEEP:	12288:DcR0s3mhdK4pAp/d3XhQ6NBoeTflnwAO3ZwZEx6X6jRkcTQsljwgf3le1EfhTsw:gasee4l/d3u6NCerCDOa0ARkP/F32cn
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.PE.L.....N.....~!.....@.....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4f6c7e
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:	0xD1177F0C [Fri Feb 28 14:19:56 2081 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	0xf4c84	0xf4e00	False	0.686369400842	data	7.15292949404	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf8000	0x5c0	0x600	False	0.425130208333	data	4.09165938354	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfa000	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 20:19:55.380009890 CEST	192.168.2.4	8.8.8.8	0x6cd1	Standard query (0)	mail.ndn.edu.lb	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:19:55.665913105 CEST	192.168.2.4	8.8.8.8	0x236e	Standard query (0)	mail.ndn.edu.lb	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:19:55.626699924 CEST	8.8.8.8	192.168.2.4	0x6cd1	No error (0)	mail.ndn.edu.lb	ndn.edu.lb		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:19:55.626699924 CEST	8.8.8.8	192.168.2.4	0x6cd1	No error (0)	ndn.edu.lb		160.153.246.81	A (IP address)	IN (0x0001)
Aug 3, 2021 20:19:55.710277081 CEST	8.8.8.8	192.168.2.4	0x236e	No error (0)	mail.ndn.edu.lb	ndn.edu.lb		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:19:55.710277081 CEST	8.8.8.8	192.168.2.4	0x236e	No error (0)	ndn.edu.lb		160.153.246.81	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 20:19:55.792501926 CEST	587	49766	160.153.246.81	192.168.2.4	220-server.insight-lb.com ESMTP Exim 4.94.2 #2 Tue, 03 Aug 2021 21:19:55 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 3, 2021 20:19:55.793375969 CEST	49766	587	192.168.2.4	160.153.246.81	EHLO 134349
Aug 3, 2021 20:19:55.820009947 CEST	587	49766	160.153.246.81	192.168.2.4	250-server.insight-lb.com Hello 134349 [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 20:19:55.820411921 CEST	49766	587	192.168.2.4	160.153.246.81	STARTTLS
Aug 3, 2021 20:19:55.850832939 CEST	587	49766	160.153.246.81	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: POSH service quotation.exe PID: 6888 Parent PID: 5784

General

Start time:	20:18:02
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\POSH service quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POSH service quotation.exe'

Imagebase:	0xb90000
File size:	1005568 bytes
MD5 hash:	FBE4C77E66F8D27264B57E4358648DE2
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: 7096 Parent PID: 6888

General

Start time:	20:18:23
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:	0x10000
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: 00000002.00000002.908110927.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.908110927.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.909617305.0000000002361000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.909617305.0000000002361000.00000004.00000001.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: 6640 Parent PID: 3424

General

Start time:	20:18:52
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:	0x620000
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: 6692 Parent PID: 6640

General

Start time:	20:18:53
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: 5872 Parent PID: 3424

General

Start time:	20:19:00
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:	0x410000
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: 6120 Parent PID: 5872

General

Start time:	20:19:01
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