ID: 458820
Sample Name: SOA.exe
Cookbook: default.jbs
Time: 19:18:35
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

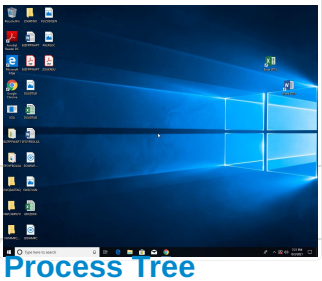
Windows Analysis Report SOA.exe

Overview

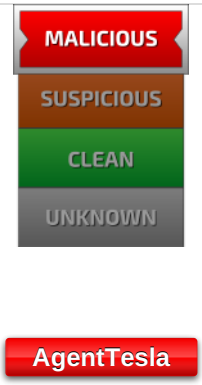
General Information

Sample Name:	SOA.exe
Analysis ID:	458820
MD5:	5fbbec81658402e.
SHA1:	af06f581f042f510..
SHA256:	deeaa200547c6ff..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

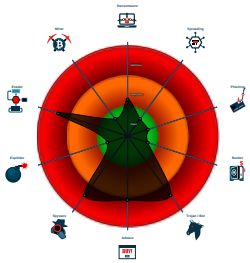


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- .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…
- Sigma detected: Suspicious Proces…
- Tries to harvest and steal Putty / Wi…

Classification



Process Tree

- **System is w10x64**
- SOA.exe (PID: 160 cmdline: 'C:\Users\user\Desktop\SOA.exe' MD5: 5FBBEC81658402EE0E3CAC046C268C2D)
  - RegSvcs.exe (PID: 5476 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- NXLun.exe (PID: 5092 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NXLun.exe (PID: 988 cmdline: 'C:\Users\user\AppData\Roaming\NXLun\NXLun.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "paola.micheli@copangroup.xyz",
  "Password": "gibson.1990",
  "Host": "us2.smtp.mailhostbox.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.503431732.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.503431732.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000C.00000002.505245817.0000000002A61000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegSvcs.exe PID: 5476	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: RegSvcs.exe PID: 5476	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.2.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

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:

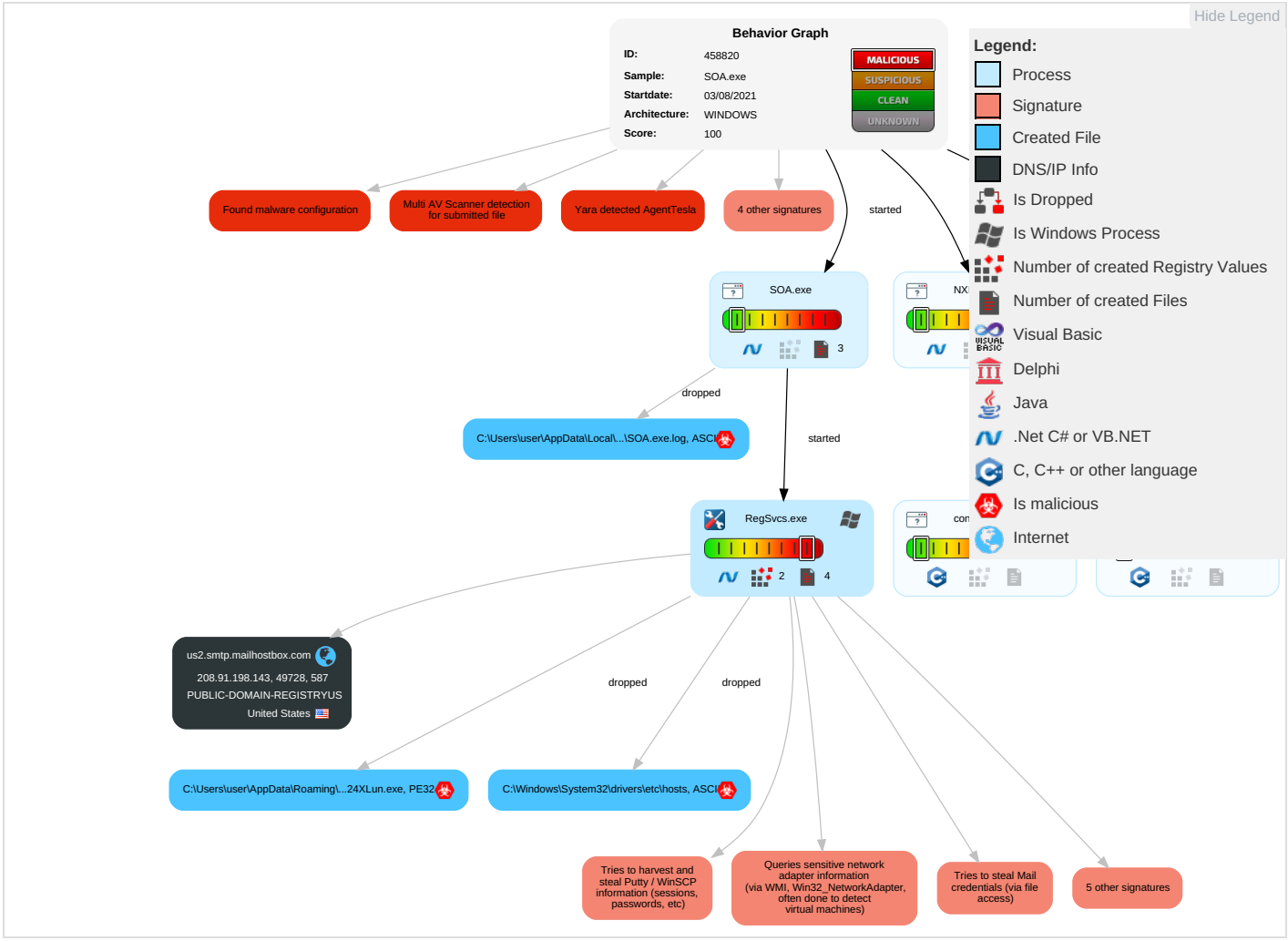
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
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	Enc Cha
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	Nor Por
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	Nor App Lay Pro
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	App Lay Pro
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 Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
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	Cor 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	App Lay
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	Wel
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 Pro

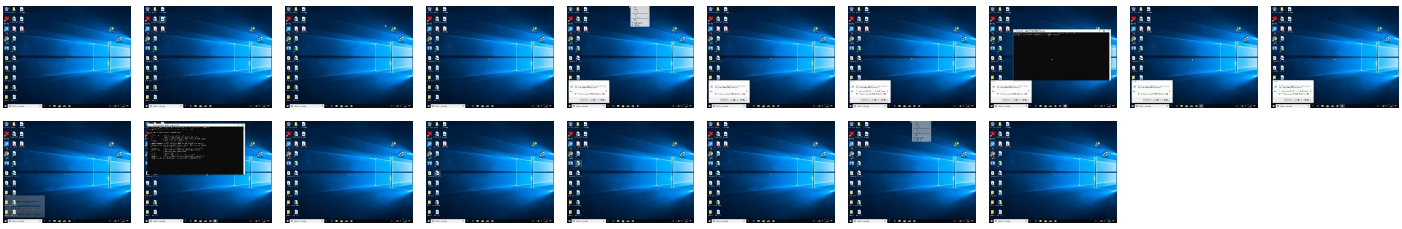
Behavior Graph



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
SOA.exe	67%	Virustotal		Browse
SOA.exe	54%	Metadefender		Browse
SOA.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SOA.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
12.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(3	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/C3	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.tiro.comFQ	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.tiro.com5	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/?3	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.commit	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.comM	0%	Avira URL Cloud	safe	
http://hFHvHh.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.tiro.comtn	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://crl.usertrust.co1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cno	0%	URL Reputation	safe	
http://https://f5KiqD21Kxl.com	0%	Avira URL Cloud	safe	
http://www.founder.c4/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn1	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.tiro.comX	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krP	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ita	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.fonts.comn_	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krll	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnf	0%	URL Reputation	safe	
http://www.fonts.comx	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://www.jiyu-kobo.co.jp/jp/Z3	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458820
Start date:	03.08.2021
Start time:	19:18:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SOA.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:	29
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@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 100% • Quality standard deviation: 0%
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
19:19:53	API Interceptor	1x Sleep call for process: SOA.exe modified
19:20:03	API Interceptor	650x Sleep call for process: RegSvcs.exe modified
19:20:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NXLun C:\Users\user\AppData\Roaming\NXLun\NXLun.exe
19:20:20	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
208.91.198.143	Invoice.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan#0068-46c3367.exe	Get hash	malicious	Browse	
	IMG-20210802-WA0587-085.exe	Get hash	malicious	Browse	
	IMG-20210802-WA0587-087.exe	Get hash	malicious	Browse	
	order.PDF.exe	Get hash	malicious	Browse	
	PURCHASE ORDER-PO-S.L 45675675.pdf.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	Pedido urgente.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Zusy.394472.4088.exe	Get hash	malicious	Browse	
	JMIRLIEMHBPEEQvrxjqCV.exe	Get hash	malicious	Browse	
	Aditi Tiwari Resume.pdf.exe	Get hash	malicious	Browse	
	NEW RFQ FROM WEB AFRITECH.doc	Get hash	malicious	Browse	
	Shipment documents pdf.exe	Get hash	malicious	Browse	
	REMITTANCE COPY.exe	Get hash	malicious	Browse	
	ok1.exe	Get hash	malicious	Browse	
	4378e6769c14e63e1b385e955ee06b93.exe	Get hash	malicious	Browse	
	HSBC PAYMENT ADVICE.exe	Get hash	malicious	Browse	
	Doc-67789845678765670987655.exe	Get hash	malicious	Browse	
	Doc-67789845678765670987654.exe	Get hash	malicious	Browse	
	invoice and payment.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	MJLkaPZomUolseU.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.MSIL.Kryptik.56a80396.11710.exe	Get hash	malicious	Browse	• 208.91.199.224
	Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan#0068-46c3367.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan#0068-46c3366.exe	Get hash	malicious	Browse	• 208.91.199.223
	IMG-20210802-WA0587-085.exe	Get hash	malicious	Browse	• 208.91.198.143
	IMG-20210802-WA0587-087.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.225
	PURCHASE ORDER PO09377 _093640_9307355_2 64378_88479_0E974.exe	Get hash	malicious	Browse	• 208.91.199.225
	order.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	RFQ #7696679TTR6F.exe	Get hash	malicious	Browse	• 208.91.199.224
	Waybill Doc_027942941.exe	Get hash	malicious	Browse	• 208.91.199.225
	Confirmaci#U00f3n de pago .exe	Get hash	malicious	Browse	• 208.91.199.224
	oBNvb4c6bg.exe	Get hash	malicious	Browse	• 208.91.199.224
	TVz86np48Z.exe	Get hash	malicious	Browse	• 208.91.199.223
	Current Vendor Payment Application .doc	Get hash	malicious	Browse	• 208.91.199.224
	XiAn Sunnstatement 27-07-2021 pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PURCHASE ORDER-PO-S.L 45675675.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	QAP 367893738 Ed 7 pcs.exe	Get hash	malicious	Browse	• 208.91.199.224
	Remittance Advise.doc	Get hash	malicious	Browse	• 208.91.199.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	QUOTATION LIST FOR NEW ORDER.exe	Get hash	malicious	Browse	• 204.11.58.233
	MJLkaPZomUolseU.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.MSIL.Kryptik.56a80396.11710.exe	Get hash	malicious	Browse	• 208.91.199.224
	Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan#0068-46c3367.exe	Get hash	malicious	Browse	• 208.91.199.224
	Scan#0068-46c3366.exe	Get hash	malicious	Browse	• 208.91.199.223
	bin.exe	Get hash	malicious	Browse	• 119.18.54.122
	IMG-20210802-WA0587-085.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG-20210802-WA0587-087.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.224
	QUOTE 04202021.exe	Get hash	malicious	Browse	• 103.21.58.16
	PURCHASE ORDER PO09377 _093640_9307355_2 64378_88479_0E974.exe	Get hash	malicious	Browse	• 208.91.199.225
	order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ #7696679TTR6F.exe	Get hash	malicious	Browse	• 208.91.199.224
	Waybill Doc_027942941.exe	Get hash	malicious	Browse	• 208.91.199.225
	Confirmaci#U00f3n de pago .exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	triage_dropped_file.exe	Get hash	malicious	Browse	• 162.222.226.11
	oBNvb4c6bg.exe	Get hash	malicious	Browse	• 208.91.199.224
	TVz86np48Z.exe	Get hash	malicious	Browse	• 208.91.199.223
	Current Vendor Payment Application .doc	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\NXLun\NXLun.exe	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	
	PO.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\SOA.exe.log	
Process:	C:\Users\user\Desktop\SOA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SOA.exe.log	
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\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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\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%
Joe Sandbox View:	• 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 • Filename: PO.exe, Detection: malicious, Browse
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
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):	7.205234682340215
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:	SOA.exe
File size:	1041920
MD5:	5fbbec81658402ee0e3cac046c268c2d
SHA1:	af06f581f042f5102bd375bf3632b462bef144d9
SHA256:	deeaa200547c6ffa325f662ec9b9ddcf0cf127826da37c2e5c514be84da26e88
SHA512:	2a6ecee547ce20f0fec92e7dca62dd34b34d4f77209df3cc1e6a1ee470f7f5f5e91b39b15059bedab1537dac3b0fde9b852e4c31f18e28f176cf0b69d48b9de0
SSDEEP:	12288:JgKyaglu6KaOUkMUweV5/d3bA8mkxlGah9+3GXvZ3nqKO1HnJGIC+7BgXfHuQ3nD:OKtaO2UJ5/d3Lmqbh025q3zLtlf/3R5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....l.....n.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ffb6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x986C96A7 [Fri Jan 13 20:08:07 2051 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	0xfdb74	0xfdc00	False	0.697750538793	data	7.21124582486	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x100000	0x5d8	0x600	False	0.429036458333	data	4.14205522772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x102000	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 19:21:30.640806913 CEST	192.168.2.5	8.8.8.8	0x7fc4	Standard query (0)	us2.smtp.mailhostbox.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 19:21:30.676964045 CEST	8.8.8.8	192.168.2.5	0x7fc4	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Aug 3, 2021 19:21:30.676964045 CEST	8.8.8.8	192.168.2.5	0x7fc4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Aug 3, 2021 19:21:30.676964045 CEST	8.8.8.8	192.168.2.5	0x7fc4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Aug 3, 2021 19:21:30.676964045 CEST	8.8.8.8	192.168.2.5	0x7fc4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

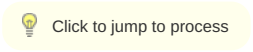
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 19:21:31.085036993 CEST	587	49728	208.91.198.143	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
Aug 3, 2021 19:21:31.085583925 CEST	49728	587	192.168.2.5	208.91.198.143	EHLO 358075
Aug 3, 2021 19:21:31.234668970 CEST	587	49728	208.91.198.143	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Aug 3, 2021 19:21:31.235749960 CEST	49728	587	192.168.2.5	208.91.198.143	STARTTLS
Aug 3, 2021 19:21:31.384911060 CEST	587	49728	208.91.198.143	192.168.2.5	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SOA.exe PID: 160 Parent PID: 5552

General

Start time:	19:19:29
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\SOA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SOA.exe'
Imagebase:	0x670000
File size:	1041920 bytes
MD5 hash:	5FBBEC81658402EE0E3CAC046C268C2D
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: 5476 Parent PID: 160

General

Start time:	19:19:54
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:	0x7b0000
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: 0000000C.00000002.503431732.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.503431732.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.505245817.0000000002A61000.00000004.00000001.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: 5092 Parent PID: 3472

General

Start time:	19:20:20
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:	0x5c0000
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: 4664 Parent PID: 5092

General

Start time:	19:20:21
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 988 Parent PID: 3472

General

Start time:	19:20:28
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:	0xe50000
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: 4500 Parent PID: 988

General

Start time:	19:20:29
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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