ID: 532705
Sample Name: Bank payment swift message.exe
Cookbook: default.jbs
Time: 16:26:02
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

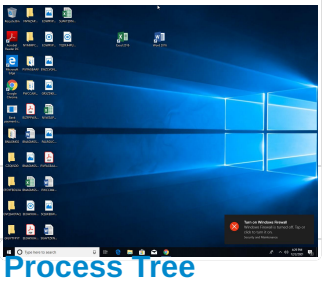
Windows Analysis Report Bank payment swift message…

Overview

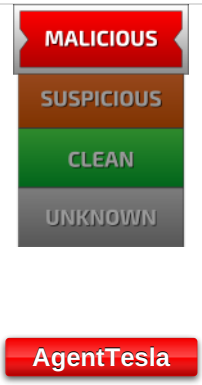
General Information

Sample Name:	Bank payment swift message.exe
Analysis ID:	532705
MD5:	8cf71f83b169db6..
SHA1:	50cde0ed5ae88e..
SHA256:	7c04ed79e65782..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

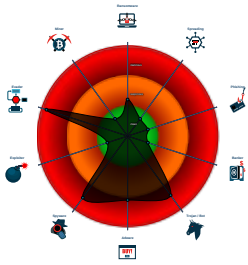


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Bank payment swift message.exe (PID: 4324 cmdline: "C:\Users\user\Desktop\Bank payment swift message.exe" MD5: 8CF71F83B169DB6428CE1345EACEC7E1)
  - RegSvcs.exe (PID: 6480 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6576 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- kprUEGC.exe (PID: 4896 cmdline: "C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- kprUEGC.exe (PID: 2144 cmdline: "C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "leell@scsgroups.com",
  "Password": "Scs@looi1007",
  "Host": "mail.scsgroups.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.303493961.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.303493961.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000000.303809538.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.303809538.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000000.302850408.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, 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

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

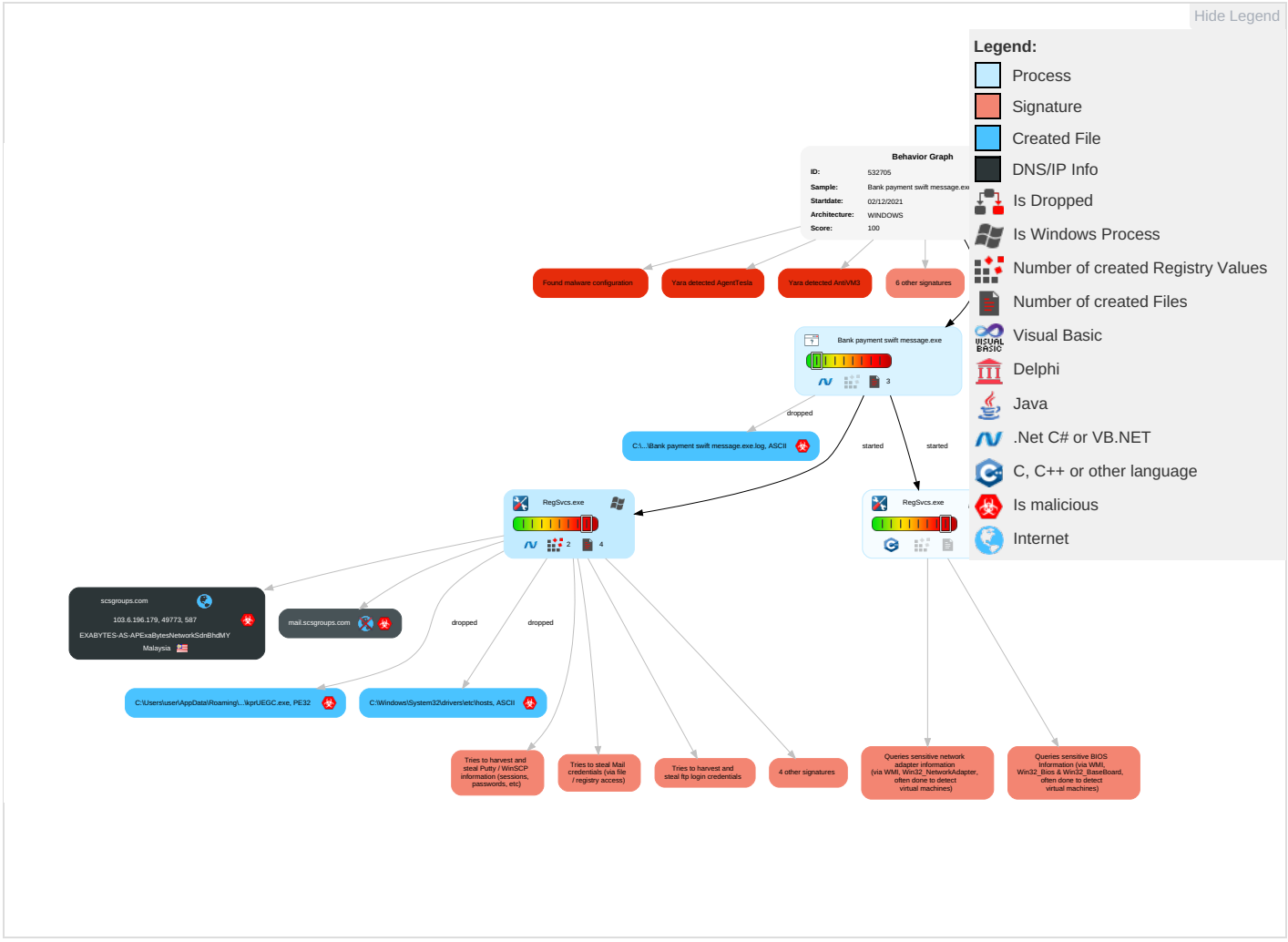
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
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
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
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

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

No Antivirus matches

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
scsgroups.com	0%	Virustotal		Browse
mail.scsgroups.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mail.scsgroups.com	0%	Virustotal		Browse
http://mail.scsgroups.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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://scsgroups.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://https://8LBhYvjS8QE2L4B.com	0%	Avira URL Cloud	safe	
http://WjMsNT.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scsgroups.com	103.6.196.179	true	true	• 0%, Virustotal, Browse	unknown
mail.scsgroups.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.6.196.179	scsgroups.com	Malaysia		46015	EXABYTES-AS-APExaBytesNetworkSdnBhdMY	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532705
Start date:	02.12.2021
Start time:	16:26:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bank payment swift message.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@9/6@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
16:27:02	API Interceptor	1x Sleep call for process: Bank payment swift message.exe modified
16:27:13	API Interceptor	776x Sleep call for process: RegSvcs.exe modified
16:27:26	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
16:27:34	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.6.196.179	Bank payment swift message.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	DOCUMENT.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	
	PURCHASE ORDER HIUK 211020 SY.exe	Get hash	malicious	Browse	
	NEW ORDER EN31628 EN31630.exe	Get hash	malicious	Browse	
	Shipping Document BL Draft.exe	Get hash	malicious	Browse	
	Payment Advice 50053945.exe	Get hash	malicious	Browse	
	QUOTATION.exe	Get hash	malicious	Browse	
	New order - C.S.I No. 0987.exe	Get hash	malicious	Browse	
	PCIPL Introduction Profile.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis44E494790094.16425.exe	Get hash	malicious	Browse	
	HMaq2KmJJD.exe	Get hash	malicious	Browse	
	2281.xls	Get hash	malicious	Browse	
	2281.xls	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
EXABYTES-AS-APExaBytesNetworkSdnBhdMY	Bank payment swift message.exe	Get hash	malicious	Browse	• 103.6.196.179
	SOA.exe	Get hash	malicious	Browse	• 103.6.196.179
	DOCUMENT.exe	Get hash	malicious	Browse	• 103.6.196.179
	Purchase order.exe	Get hash	malicious	Browse	• 103.6.196.179
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	• 103.6.196.179
	RFQ#00890.exe	Get hash	malicious	Browse	• 110.4.45.145
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	• 103.6.196.179
	SOA.exe	Get hash	malicious	Browse	• 103.6.196.179
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	• 103.6.196.179
	Linux_x86	Get hash	malicious	Browse	• 103.6.196.36
	PURCHASE ORDER HIUK 211020 SY.exe	Get hash	malicious	Browse	• 103.6.196.179
	order PO6766.exe	Get hash	malicious	Browse	• 110.4.45.145
	NEW ORDER EN31628 EN31630.exe	Get hash	malicious	Browse	• 103.6.196.179
	Shipping Document BL Draft.exe	Get hash	malicious	Browse	• 103.6.196.179
	Payment Advice 50053945.exe	Get hash	malicious	Browse	• 103.6.196.179
	QUOTATION.exe	Get hash	malicious	Browse	• 103.6.196.179
	New order - C.S.I No. 0987.exe	Get hash	malicious	Browse	• 103.6.196.179
	PCIPL Introduction Profile.exe	Get hash	malicious	Browse	• 103.6.196.179
	SecuriteInfo.com.Artemis44E494790094.16425.exe	Get hash	malicious	Browse	• 103.6.196.179
	NEW ORDER.exe	Get hash	malicious	Browse	• 137.59.109.172

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	SALES INVOICE-CINV-00095891.exe	Get hash	malicious	Browse	
	JSGD-09873673893873.exe	Get hash	malicious	Browse	
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	Bank payment swift message.exe	Get hash	malicious	Browse	
	PAYMENT PROOF.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	DOCUMENT.exe	Get hash	malicious	Browse	
	swift copy.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	
	INVOICE.exe	Get hash	malicious	Browse	
	IMGLM_09846456748-4098476748464.exe	Get hash	malicious	Browse	
	remitted payment.exe	Get hash	malicious	Browse	
	PAYMENT SLIP OF SY21.exe	Get hash	malicious	Browse	
	request quotation.exe	Get hash	malicious	Browse	
	swift copy.exe	Get hash	malicious	Browse	
	BCAVT_C0938763-398763693863.exe	Get hash	malicious	Browse	
	DOC.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Bank payment swift message.exe.log

Process:	C:\Users\user\Desktop\Bank payment swift message.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Bank payment swift message.exe.log	
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, 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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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:	high, 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\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SALES INVOICE-CINV-00095891.exe, Detection: malicious, Browse • Filename: JSGD-09873673893873.exe, Detection: malicious, Browse • Filename: DHL SHIPMENT NOTIFICATION 284748395PD.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: Bank payment swift message.exe, Detection: malicious, Browse • Filename: PAYMENT PROOF.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: DOCUMENT.exe, Detection: malicious, Browse • Filename: swift copy.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse • Filename: Purchase order.exe, Detection: malicious, Browse • Filename: PAYMENT SLIP OF SY21.exe, Detection: malicious, Browse • Filename: INVOICE.exe, Detection: malicious, Browse • Filename: IMGLM_09846456748-4098476748464.exe, Detection: malicious, Browse • Filename: remitted payment.exe, Detection: malicious, Browse • Filename: PAYMENT SLIP OF SY21.exe, Detection: malicious, Browse • Filename: request quotation.exe, Detection: malicious, Browse • Filename: swift copy.exe, Detection: malicious, Browse • Filename: BCAVT_C0938763-398763693863.exe, Detection: malicious, Browse • Filename: DOC.exe, Detection: malicious, Browse

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
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):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.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):	7.782175785902415
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Bank payment swift message.exe
File size:	481280
MD5:	8cf71f83b169db6428ce1345eacec7e1
SHA1:	50cde0ed5ae88e15fc6a190216f767c61014261f
SHA256:	7c04ed79e657827d9ed17fc6f50e51a5818bf9b7db804691dee2470d5371162e

General

SHA512:	e66d9f4dfa5bb8bd30182549b11b0a78345696d48ab4f03c0571081ea63ac3005a5681ebacf50981b3d359c9fd9c3c911ea254794ba8dfa63ed93c56e9f7d1ea
SSDEEP:	12288:1qgpfvuXCk4O2kg7RNDvXTmTJXQfyNlCkOl:gCk4Sg1dXwBvNl6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....N.....m... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x476dbe
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:	0xF5F8E4E2 [Sat Oct 9 01:44:02 2100 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	0x74dc4	0x74e00	False	0.88877214238	data	7.79400294438	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x4d8	0x600	False	0.375651041667	data	3.72627161824	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7a000	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
Dec 2, 2021 16:28:40.785038948 CET	192.168.2.3	8.8.8.8	0x7d2c	Standard query (0)	mail.scsgroups.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:28:40.932601929 CET	192.168.2.3	8.8.8.8	0x2040	Standard query (0)	mail.scsgroups.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 16:28:40.921739101 CET	8.8.8.8	192.168.2.3	0x7d2c	No error (0)	mail.scsgroups.com	scsgroups.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:28:40.921739101 CET	8.8.8.8	192.168.2.3	0x7d2c	No error (0)	scsgroups.com		103.6.196.179	A (IP address)	IN (0x0001)
Dec 2, 2021 16:28:41.081876993 CET	8.8.8.8	192.168.2.3	0x2040	No error (0)	mail.scsgroups.com	scsgroups.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:28:41.081876993 CET	8.8.8.8	192.168.2.3	0x2040	No error (0)	scsgroups.com		103.6.196.179	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 16:28:41.653023005 CET	587	49773	103.6.196.179	192.168.2.3	220-xl-galactus.mschosting.com ESMTP Exim 4.94.2 #2 Thu, 02 Dec 2021 23:28:40 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 2, 2021 16:28:41.653459072 CET	49773	587	192.168.2.3	103.6.196.179	EHLO 562258
Dec 2, 2021 16:28:41.918298960 CET	587	49773	103.6.196.179	192.168.2.3	250-xl-galactus.mschosting.com Hello 562258 [84.17.52.65] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Dec 2, 2021 16:28:41.918554068 CET	49773	587	192.168.2.3	103.6.196.179	STARTTLS
Dec 2, 2021 16:28:42.184674025 CET	587	49773	103.6.196.179	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Bank payment swift message.exe PID: 4324 Parent PID: 4960

General

Start time:	16:27:00
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Bank payment swift message.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Bank payment swift message.exe"
Imagebase:	0x670000
File size:	481280 bytes
MD5 hash:	8CF71F83B169DB6428CE1345EACEC7E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.306719644.0000000003B29000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.306719644.0000000003B29000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.305709842.0000000002B21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.305889560.0000000002C10000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 6480 Parent PID: 4324

General

Start time:	16:27:03
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x360000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6576 Parent PID: 4324

General

Start time:	16:27:04
Start date:	02/12/2021
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:	0x7c0000
File size:	45152 bytes

MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.303493961.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.303493961.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.303809538.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.303809538.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.302850408.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.302850408.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.558202775.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.558202775.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.303165752.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.303165752.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.559822771.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.559822771.0000000002AE1000.00000004.00000001.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: kprUEGC.exe PID: 4896 Parent PID: 3352

General

Start time:	16:27:34
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe"
Imagebase:	0x4f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
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: 1244 Parent PID: 4896

General

Start time:	16:27:35
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kprUEGC.exe PID: 2144 Parent PID: 3352

General

Start time:	16:27:42
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe"
Imagebase:	0x8c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 1492 Parent PID: 2144

General

Start time:	16:27:42

Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis