ID: 337336
Sample Name:
SecuriteInfo.com.generic.ml.32161
Cookbook: default.jbs
Time: 10:51:43
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

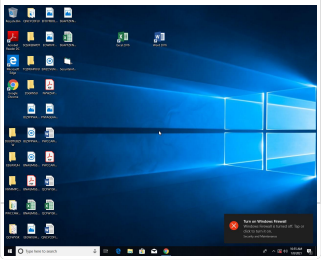
Analysis Report SecuriteInfo.com.generic.ml.32161

Overview

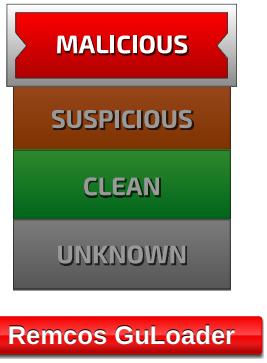
General Information

Sample Name:	SecuriteInfo.com.generic.ml.32161 (renamed file extension from 32161 to exe)
Analysis ID:	337336
MD5:	0640f43c412f8f2…
SHA1:	f07e9e5e618b14b.
SHA256:	1664c6a330c5b3..
Tags:	GuLoader

Most interesting Screenshot:



Detection

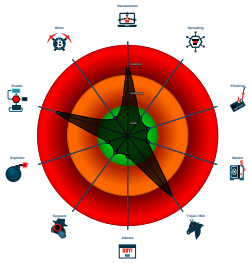


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Sigma detected: Remcos
- Yara detected GuLoader
- Connects to many ports of the same…
- Contains functionality to hide a threa…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Writes to foreign memory regions
- Yara detected VB6 Downloader Gen…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.generic.ml.exe (PID: 908 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: 0640F43C412F8F2C3BF6E1B9139DB1D0)
  - ieinstal.exe (PID: 6588 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6612 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6640 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6680 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6724 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6776 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6848 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6908 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6988 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 7012 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 7056 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ielowutil.exe (PID: 7084 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe' MD5: D1F5C3244A69511CAC88009B71884A71)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.570071221.0000000002AD1000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000000.00000002.313168282.0000000000409000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0xce8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000000.00000000.205779909.0000000000409000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0xce8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB

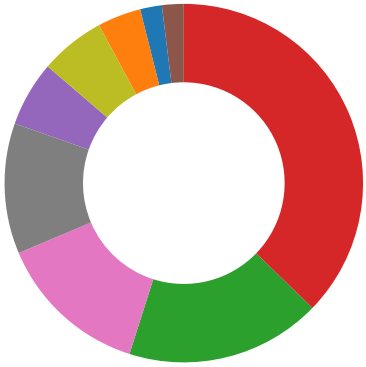
Source	Rule	Description	Author	Strings
Process Memory Space: ielowutil.exe PID: 7084	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: SecuriteInfo.com.generic.ml.exe PID: 908	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Remcos

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Connects to many ports of the same IP (likely port scanning)

System Summary:

Malicious sample detected (through community Yara rule)

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

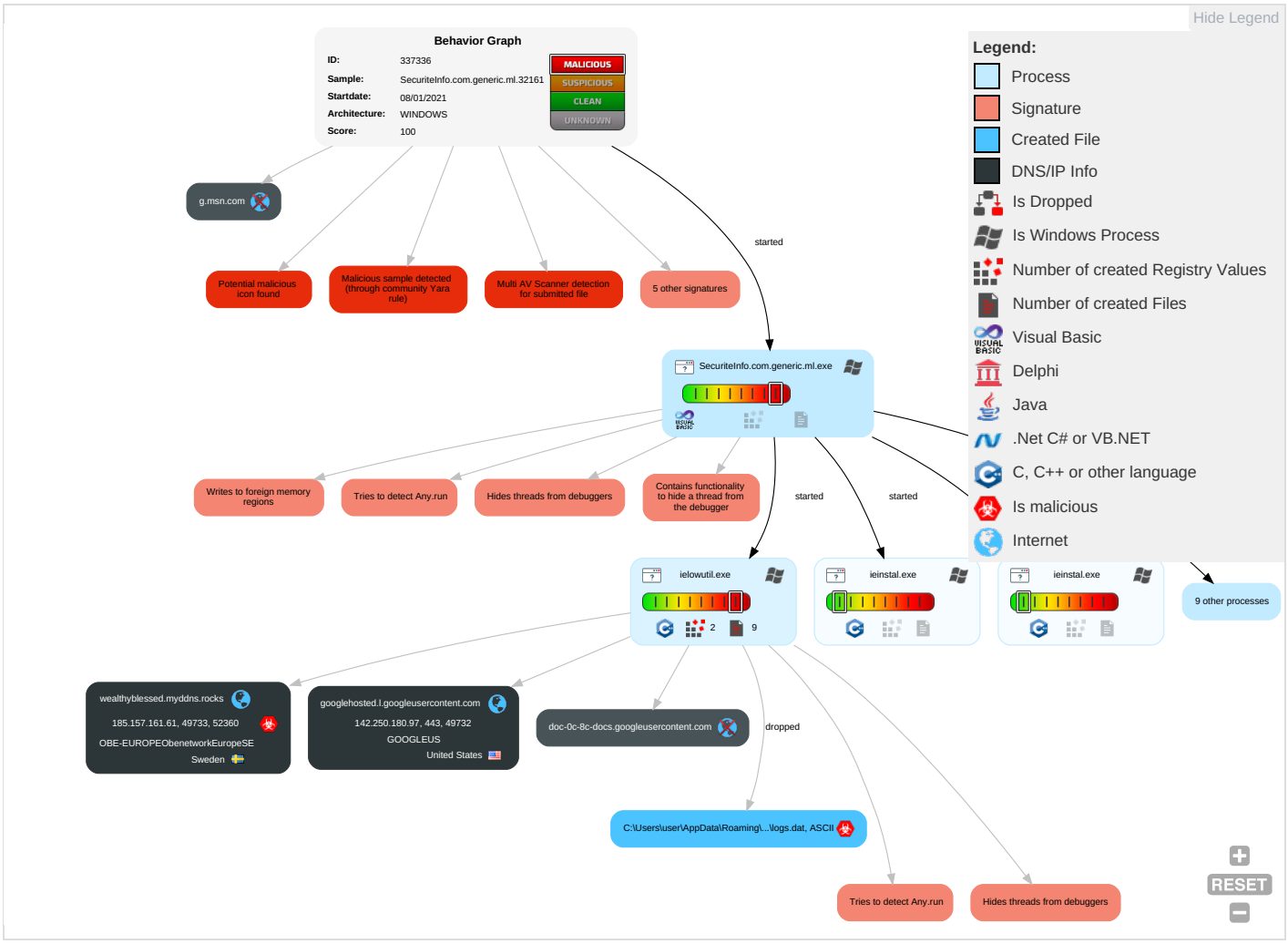
HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

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	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 4 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

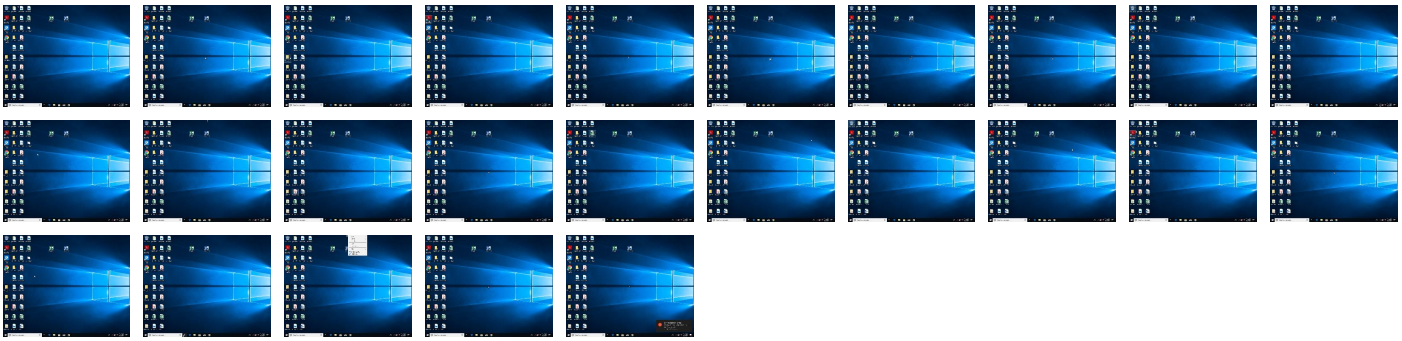
Behavior Graph



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.generic.ml.exe	11%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://pki.goog/r	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2	0%	Avira URL Cloud	safe	

Domains and IPs

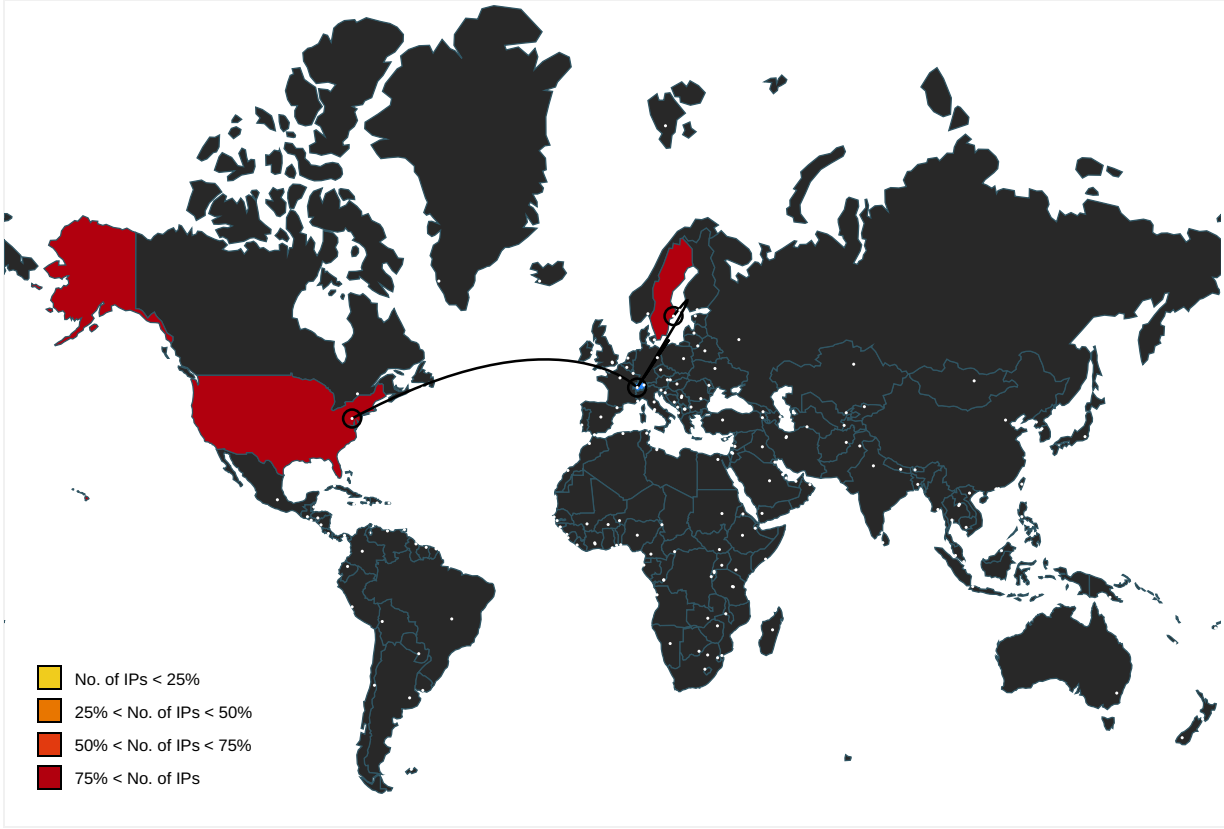
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthyblessed.myddns.rocks	185.157.161.61	true	true		unknown
googlehosted.l.googleusercontent.com	142.250.180.97	true	false		high
g.msn.com	unknown	unknown	false		high
doc-0c-8c-docs.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr2/GTS1O1.crt0	ielowutil.exe, 00000016.00000002.571131966.0000000002FAE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/r	ielowutil.exe, 00000016.00000002.571131966.0000000002FAE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	ielowutil.exe, 00000016.00000003.540935394.0000000002FAE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	ielowutil.exe, 00000016.00000003.540935394.0000000002FAE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	ielowutil.exe, 00000016.00000003.540935394.0000000002FAE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	ielowutil.exe, 00000016.00000002.571131966.0000000002FAE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	ielowutil.exe, 00000016.00000002.571131966.0000000002FAE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2	ielowutil.exe, 00000016.00000002.571131966.0000000002FAE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.161.61	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
142.250.180.97	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337336
Start date:	08.01.2021
Start time:	10:51:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.generic.ml.32161 (renamed file extension from 32161 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:	40
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.rans.troj.evad.winEXE@25/1@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.7% (good quality ratio 1.5%) • Quality average: 47.6% • Quality standard deviation: 19.1%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 168.61.161.212, 104.43.139.144, 40.88.32.150, 104.79.90.110, 40.126.1.130, 20.190.129.133, 20.190.129.24, 20.190.129.17, 40.126.1.145, 20.190.129.160, 20.190.129.19, 20.190.129.2, 51.104.139.180, 92.122.213.247, 92.122.213.194, 8.253.207.120, 8.253.204.120, 67.27.157.126, 67.26.73.254, 8.248.149.254, 142.250.180.78, 20.54.26.129, 84.53.167.113, 51.11.168.160, 52.142.114.176, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, login.live.com, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
10:53:21	API Interceptor	1065x Sleep call for process: ielowutil.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.157.161.61	New PO.doc	Get hash	malicious	Browse	
142.250.180.97	New PO.doc	Get hash	malicious	Browse	
	http://down10d.zol.com.cn/zoldownload/fangsong_GB2312@81_432727.exe	Get hash	malicious	Browse	
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	
	http://kubecloud.com	Get hash	malicious	Browse	
	http://https://blog.dericoin.com/wp-includes/shell/ivd/office/office/voicemail/index.php	Get hash	malicious	Browse	
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	
	jfuoevj.exe	Get hash	malicious	Browse	
	http://subreqxserver1132.azurewebsites.net	Get hash	malicious	Browse	
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	
	http://https://wfuwdbjwquoiynfb-dot-tundasma.el.r.appspot.com/#test@test.com	Get hash	malicious	Browse	
	r0u.exe	Get hash	malicious	Browse	
	r0u.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
googlehosted.l.googleusercontent.com	New PO.doc	Get hash	malicious	Browse	• 142.250.180.97
	http://down10d.zol.com.cn/zoldownload/fangsong_GB2312@81_432727.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 142.250.180.97
	http://kubecloud.com	Get hash	malicious	Browse	• 142.250.180.97
	http://https://blog.dericoin.com/wp-includes/shell/ivd/office/office/voicemail/index.php	Get hash	malicious	Browse	• 142.250.180.97
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 142.250.180.97
	jfuoevj.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://subreqxserver1132.azurewebsites.net	Get hash	malicious	Browse	• 142.250.180.97
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	• 142.250.180.97
	http://https://wfuwdbjwquoiynfb-dot-tundasma.el.r.appspot.com/#test@test.com	Get hash	malicious	Browse	• 142.250.180.97
	r0u.exe	Get hash	malicious	Browse	• 142.250.180.97
	r0u.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://bit.ly/3nlGvk0	Get hash	malicious	Browse	• 216.58.206.33
	http://fokpsrhpqilmgun.65kjh455kh566gf.camdvr.org	Get hash	malicious	Browse	• 216.58.206.33
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 216.58.206.33
	#Ud83d#Udcde_8360.htm	Get hash	malicious	Browse	• 216.58.215.225
	Westernsouthernlife8PG5-YSGL2K-TVU4.htm	Get hash	malicious	Browse	• 216.58.215.225
	http://https://alijafari6.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 216.58.215.225
	zsmcirs.exe	Get hash	malicious	Browse	• 216.58.215.225
	http://https://grantsvillemd.xyz/amlsbC5tY2dydWRlckB3ZXN0ZXJuc291dGhlcm4uY29t	Get hash	malicious	Browse	• 216.58.215.225
wealthyblessed.myddns.rocks	New PO.doc	Get hash	malicious	Browse	• 185.157.161.61

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	New PO.doc	Get hash	malicious	Browse	• 185.157.161.61
	89GsVCJAXv.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	dpR3o92MH1.exe	Get hash	malicious	Browse	• 185.157.162.81
	0qNSJXB8nG.exe	Get hash	malicious	Browse	• 185.157.162.81
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 185.157.161.86
	7w7LwD8bqe.exe	Get hash	malicious	Browse	• 185.157.162.81
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	ptoovvKZ80.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	EnJsj6nuD4.exe	Get hash	malicious	Browse	• 185.157.162.81
	AdviceSlip.xls	Get hash	malicious	Browse	• 217.64.149.169

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	50404868-c352-422f-a608-7fd64b335eec.exe	Get hash	malicious	Browse	• 185.157.161.86
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
GOOGLEUS	FTH2004-005.exe	Get hash	malicious	Browse	• 34.102.136.180
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 35.241.57.45
	Confirm!!!..exe	Get hash	malicious	Browse	• 34.102.136.180
	S4P1JiBZIZxvtFR.exe	Get hash	malicious	Browse	• 34.102.136.180
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 35.241.57.45
	inv.exe	Get hash	malicious	Browse	• 34.102.136.180
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 34.102.136.180
	PO(2021.01.08).exe	Get hash	malicious	Browse	• 34.102.136.180
	2143453.exe	Get hash	malicious	Browse	• 35.213.137.208
	order.exe	Get hash	malicious	Browse	• 34.102.136.180
	New PO.doc	Get hash	malicious	Browse	• 142.250.180.97
	http://down10d.zol.com.cn/zoldownload/fangsong_GB2312@81_432727.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://https://1drv.ms:443/o/s!BAXL7VqGJe6lg0eKk2MZcT_c29ga?e=Qdftz9F3oESsQIuV76Ppsw&at=9	Get hash	malicious	Browse	• 130.211.19.189
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 216.58.198.1
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 142.250.180.97
	http://kubecloud.com	Get hash	malicious	Browse	• 142.250.180.97
	http://https://blog.dericoin.com/wp-includes/shell/ivd/office/office/voicemail/index.php	Get hash	malicious	Browse	• 142.250.180.97
	http://message.mydopweb.com	Get hash	malicious	Browse	• 216.58.198.33
	2.apk	Get hash	malicious	Browse	• 142.250.180.74
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 142.250.180.97

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	home.css.ps1	Get hash	malicious	Browse	• 142.250.180.97
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 142.250.180.97
	36.exe	Get hash	malicious	Browse	• 142.250.180.97
	Buran.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 142.250.180.97
	http://https://survey.alchemer.com/s3/6130663/Check-11-Payment	Get hash	malicious	Browse	• 142.250.180.97
	http://https://smlfinance.com/wp-content/uploads/2021/DHL2021/MARKET/	Get hash	malicious	Browse	• 142.250.180.97
	atikmdag-patcher 1.4.8.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://https://atacadaodocompensado.com.br/office356.com-RD163	Get hash	malicious	Browse	• 142.250.180.97
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 142.250.180.97
	jfuoevj.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://https://blog.dericoin.com/wp-includes/shell/ivd/Office/office/voicemail/index.php	Get hash	malicious	Browse	• 142.250.180.97
	http://https://wqi69130.mfs.gg/099mmYI	Get hash	malicious	Browse	• 142.250.180.97
	PolicyUpdate.htm	Get hash	malicious	Browse	• 142.250.180.97
	http://https://1drv.ms/u/s!AmqlOnt-7_dxdENKsoSwOCjxG_Q?e=3ZrXeG	Get hash	malicious	Browse	• 142.250.180.97
	http://https://webmail-4fd4rvt.web.app/?emailtoken=jmahler@vocera.com&domain=vocera.com	Get hash	malicious	Browse	• 142.250.180.97
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 142.250.180.97
	202101041.htm	Get hash	malicious	Browse	• 142.250.180.97
	http://https://moorparklancssch-my.sharepoint.com/:o:/g/personal/16willcocks_pupils_moorpark_mp/EpuojDvAqLNHlYVejf5zx0kBqAdkUjR2VgNWcoUhvcauDg?e=Th0p8a	Get hash	malicious	Browse	• 142.250.180.97
	http://https://bit.ly/3ba3hZS	Get hash	malicious	Browse	• 142.250.180.97

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.673971569609487
Encrypted:	false
SSDEEP:	3:ttU3aWfXbArA4RXMRPHv31aeo:tmlSXqdHv3lP
MD5:	6FDD9F8E355305C4B08519E72F85F3DB
SHA1:	753E7BD3D8C8752A954BCCDB47CC1A6670F64145
SHA-256:	3DD190CA2C952F72F77C584BCD302523E99ABB5990FB43285D5A6C12EF9C2159
SHA-512:	AC7BEA4611D75E5419143CA81044E3A825785D730E647563B2D131010BA3EF987396E6A0F11907201B53E1810A973F8197E58FE003069A2CB0235805F6F03E5C
Malicious:	**true**
Reputation:	low
Preview:	..[2021/01/08 10:53:21 Offline Keylogger Started]....[Program Manager]..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.76607868664825
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.generic.ml.exe
File size:	73728
MD5:	0640f43c412f8f2c3bf6e1b9139db1d0
SHA1:	f07e9e5e618b14b0dd5478cb2a26f42096a10e1d
SHA256:	1664c6a330c5b318458518ea71b2a9995a91c79281a050 278c3aa2388663a986
SHA512:	753029891e9db39d072cce14dd552ef313479ea0cff2e4c 3a5591bbf045174ea474e2651c8bdbed5ca30429852f4d2 8a5126fe99bfcaf9aa9daec30ac46f0a05
SSDEEP:	768:iy6BPW3W6LV4htQ0HOwdHegY9f8BlqvrA23WPlQ bu3FEtQKqECzHiFN1gx:iLBC5Jzwd+n9f8Wj73WP7EiK qlC0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L...J..G.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012d4

General

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:	0x47B5AC4A [Fri Feb 15 15:14:18 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:	a58452980f47253c6c85d2302c371765

Entrypoint Preview

Instruction
push 004098F4h
call 00007F947CE0CDA5h
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
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push es
pop ebp
jne 00007F947CE0CD74h
xchg eax, ebx
sbb byte ptr [ebp+48h], cl
mov byte ptr [edx+08h], ch
inc ebx
xchg eax, ebx
mov esi, 0000FFBBh
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc ecx
add byte ptr [esi+42018250h], al
inc ecx
inc edi
inc esp
dec ecx
add byte ptr [esi+00h], ch
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
and eax, EE2DD2B6h
or dword ptr [esi+05874930h], 54h
sbb cl, byte ptr [esi]
xchg eax, edx
insb
popfd
xchg eax, ecx
jo 00007F947CE0CDE6h

Instruction
out B6h, al
adc dword ptr [eax+44068A47h], eax
stosd
sub ah, bh
and al, byte ptr [ecx+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
sub al, 85h
add byte ptr [eax], al
inc edi
add byte ptr [eax], al
add byte ptr [eax], al
add eax, 544C4100h
push edx
push ebp
add byte ptr [53000A01h], cl
je 00007F947CE0CE21h
jo 00007F947CE0CE18h
jne 00007F947CE0CE24h
bound esi, dword ptr [ebp+38h]
add byte ptr [ecx], bl
add dword ptr [eax], eax
inc edx
add byte ptr [edx], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf414	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11000	0x8e4	.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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xbc	.text

Name	Virtual Address	Virtual Size	Is in Section
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	0xe7c4	0xf000	False	0.3900390625	data	5.3469676548	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0xa0c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x8e4	0x1000	False	0.166748046875	data	1.92463381633	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x117b4	0x130	data		
RT_ICON	0x114cc	0x2e8	data		
RT_ICON	0x113a4	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x11374	0x30	data		
RT_VERSION	0x11150	0x224	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, __vbaFpI4, _CIatan, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0404 0x04b0
InternalName	Indk
FileVersion	1.00
CompanyName	Double Fine Productions
ProductName	pedersup
ProductVersion	1.00
OriginalFilename	Indk.exe

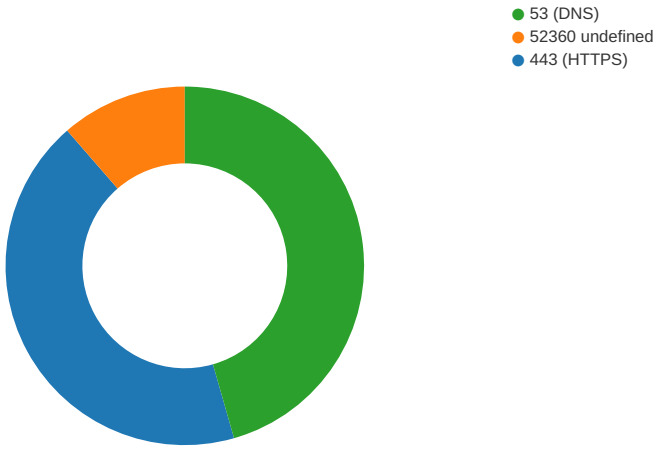
Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution

Total Packets: 79



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 10:53:20.766922951 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.823081017 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:20.823168039 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.823437929 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.879442930 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:20.895345926 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:20.895401001 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:20.895416975 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.895440102 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:20.895452023 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.895477057 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:20.895482063 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.895606995 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.912841082 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.968964100 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:20.969053030 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:20.969628096 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.031261921 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.261328936 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.261408091 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.261425972 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.261464119 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.261499882 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.261537075 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.261557102 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.261580944 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.265063047 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.265103102 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.265171051 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.268974066 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.269012928 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.269201994 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.272942066 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.272984028 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.273461103 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.276855946 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.276897907 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.276936054 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.276978016 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.280827045 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.280865908 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.280909061 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.280947924 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.318664074 CET	443	49732	142.250.180.97	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 10:53:21.318722010 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.318962097 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.320337057 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.320380926 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.320449114 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.324271917 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.324310064 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.324363947 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.328182936 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.328222990 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.328283072 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.328294992 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.332104921 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.332146883 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.332258940 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.336051941 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.336093903 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.336116076 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.336188078 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.340054989 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.340095997 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.340145111 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.340207100 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.343859911 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.343898058 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.346590996 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.347810030 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.347856998 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.348001957 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.351386070 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.351429939 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.351514101 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.354980946 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.355031013 CET	443	49732	142.250.180.97	192.168.2.3
Jan 8, 2021 10:53:21.355355024 CET	49732	443	192.168.2.3	142.250.180.97
Jan 8, 2021 10:53:21.642402887 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:21.960416079 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:21.963282108 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:21.968240023 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:22.430535078 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:22.432693005 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:22.845890045 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:27.740245104 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:27.743638039 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:28.462609053 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:28.585475922 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:29.310122967 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:32.850227118 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:32.854650974 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:33.230793953 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:37.946436882 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:37.951366901 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:38.315107107 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:43.060806036 CET	52360	49733	185.157.161.61	192.168.2.3
Jan 8, 2021 10:53:43.065222025 CET	49733	52360	192.168.2.3	185.157.161.61
Jan 8, 2021 10:53:43.425030947 CET	52360	49733	185.157.161.61	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 10:52:28.529969931 CET	65110	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:28.591248035 CET	53	65110	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:29.777122021 CET	58361	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:29.825268984 CET	53	58361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 10:52:32.966675043 CET	63492	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:33.017491102 CET	53	63492	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:33.901746988 CET	60831	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:33.952558994 CET	53	60831	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:34.893409014 CET	60100	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:34.944257975 CET	53	60100	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:37.457941055 CET	53195	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:37.506099939 CET	53	53195	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:38.394639969 CET	50141	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:38.445633888 CET	53	50141	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:39.329952955 CET	53023	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:39.377959013 CET	53	53023	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:40.264322996 CET	49563	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:40.312146902 CET	53	49563	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:41.068795919 CET	51352	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:41.116837025 CET	53	51352	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:42.013433933 CET	59349	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:42.061342955 CET	53	59349	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:43.037942886 CET	57084	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:43.085737944 CET	53	57084	8.8.8.8	192.168.2.3
Jan 8, 2021 10:52:43.950128078 CET	58823	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:52:43.998193026 CET	53	58823	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:00.657679081 CET	57568	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:00.715337992 CET	53	57568	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:09.494474888 CET	50540	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:09.545334101 CET	53	50540	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:09.948648930 CET	54366	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:09.997792006 CET	53	54366	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:16.816397905 CET	53034	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:16.872641087 CET	53	53034	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:17.719058037 CET	57762	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:17.767122030 CET	53	57762	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:19.823319912 CET	55435	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:19.879618883 CET	53	55435	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:20.698334932 CET	50713	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:20.765464067 CET	53	50713	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:21.430490971 CET	56132	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:21.639633894 CET	53	56132	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:29.345299959 CET	58987	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:29.412123919 CET	53	58987	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:43.837730885 CET	56579	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:43.896121979 CET	53	56579	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:45.281579018 CET	60633	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:45.329572916 CET	53	60633	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:46.991930008 CET	61292	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:47.056533098 CET	53	61292	8.8.8.8	192.168.2.3
Jan 8, 2021 10:53:48.817679882 CET	63619	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:53:48.874207020 CET	53	63619	8.8.8.8	192.168.2.3
Jan 8, 2021 10:54:20.013230085 CET	64938	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:54:21.097022057 CET	64938	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:54:22.108501911 CET	64938	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:54:22.158987999 CET	53	64938	8.8.8.8	192.168.2.3
Jan 8, 2021 10:54:24.428479910 CET	61946	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:54:24.487639904 CET	53	61946	8.8.8.8	192.168.2.3
Jan 8, 2021 10:55:18.426589966 CET	64910	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:55:18.534686089 CET	53	64910	8.8.8.8	192.168.2.3
Jan 8, 2021 10:55:20.367820024 CET	52123	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:55:20.427015066 CET	53	52123	8.8.8.8	192.168.2.3
Jan 8, 2021 10:55:21.083848953 CET	56130	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:55:21.193069935 CET	53	56130	8.8.8.8	192.168.2.3
Jan 8, 2021 10:55:21.646823883 CET	56338	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:55:21.703259945 CET	53	56338	8.8.8.8	192.168.2.3
Jan 8, 2021 10:55:22.222898960 CET	59420	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:55:22.279115915 CET	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 10:55:22.721251011 CET	58784	53	192.168.2.3	8.8.8.8
Jan 8, 2021 10:55:22.777802944 CET	53	58784	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 10:53:20.698334932 CET	192.168.2.3	8.8.8.8	0x6f30	Standard query (0)	doc-0c-8c-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 8, 2021 10:53:21.430490971 CET	192.168.2.3	8.8.8.8	0xdb7c	Standard query (0)	wealthyblessed.myddns.rocks	A (IP address)	IN (0x0001)
Jan 8, 2021 10:53:46.991930008 CET	192.168.2.3	8.8.8.8	0x6fea	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 8, 2021 10:53:09.545334101 CET	8.8.8.8	192.168.2.3	0x8434	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 8, 2021 10:53:20.765464067 CET	8.8.8.8	192.168.2.3	0x6f30	No error (0)	doc-0c-8c-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 8, 2021 10:53:20.765464067 CET	8.8.8.8	192.168.2.3	0x6f30	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.97	A (IP address)	IN (0x0001)
Jan 8, 2021 10:53:21.639633894 CET	8.8.8.8	192.168.2.3	0xdb7c	No error (0)	wealthyblessed.myddns.rocks		185.157.161.61	A (IP address)	IN (0x0001)
Jan 8, 2021 10:53:47.056533098 CET	8.8.8.8	192.168.2.3	0x6fea	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 8, 2021 10:53:20.895477057 CET	142.250.180.97	443	192.168.2.3	49732	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

- SecuriteInfo.com.generic.ml.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe

System Behavior

Analysis Process: SecuriteInfo.com.generic.ml.exe PID: 908 Parent PID: 5804

General

Start time:	10:52:32
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	0640F43C412F8F2C3BF6E1B9139DB1D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.313168282.0000000000409000.00000020.00020000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000000.205779909.0000000000409000.00000020.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: 6588 Parent PID: 908

General

Start time:	10:53:08
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes

MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6612 Parent PID: 908

General

Start time:	10:53:08
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6640 Parent PID: 908

General

Start time:	10:53:08
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6680 Parent PID: 908

General

Start time:	10:53:09
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6724 Parent PID: 908

General

Start time:	10:53:09
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6776 Parent PID: 908

General

Start time:	10:53:09
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6848 Parent PID: 908

General

Start time:	10:53:10
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6908 Parent PID: 908

General

Start time:	10:53:10
Start date:	08/01/2021

Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6988 Parent PID: 908

General

Start time:	10:53:10
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 7012 Parent PID: 908

General

Start time:	10:53:11
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 7056 Parent PID: 908

General

Start time:	10:53:11
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0x3c0000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true

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

Analysis Process: ielowutil.exe PID: 7084 Parent PID: 908

General

Start time:	10:53:11
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.exe'
Imagebase:	0xa80000
File size:	221184 bytes
MD5 hash:	D1F5C3244A69511CAC88009B71884A71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000016.00000002.570071221.0000000002AD1000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2AD2F83	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2AD2F83	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2AD2F83	InternetOpenUrlA
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	2AD2F83	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2AD2F83	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2AD2F83	InternetOpenUrlA
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40564C	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\remcos\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	2	412D99	CreateFileW
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40564C	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\remcos\logs.dat	unknown	51	0d 0a 5b 32 30 32 31 2f 30 31 2f 30 38 20 31 30 3a 35 33 3a 32 31 20 4f 66 66 6c 69 6e 65 20 4b 65 79 6c 6f 67 67 65 72 20 53 74 61 72 74 65 64 5d 0d 0a	..[2021/01/08 10:53:21 Offline Keylogger Started]..	success or wait	2	412DCC	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-DPTVOE\	success or wait	1	40B71B	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-DPTVOE	exepath	binary	A0 52 98 BB BE 5D 96 1A 66 5B 05 E1 86 87 86 1B 4D 4A 3F 0C 2C 7E 31 CF 4D 77 66 9A 1F E3 5C E5 22 C2 37 A4 62 3F 17 D0 32 DD F4 58 AA 08 5F 96 2D 2E 69 A5 F9 89 7F D5 9F 2C 69 B7 D2 6B C2 35 E5 10 14 B1 97 AF 32 53 F8 DE 66 7E EF BD 1F 66 87 A0 9D 36 6E 86 00 38 94 E4 DB 58 BA AA C9 7A 18 62 D9 C6 7D E8 3D 22 67 A1 8B 89 62 8E	success or wait	1	40B747	RegSetValueExA
HKEY_CURRENT_USER\Software\Remcos-DPTVOE	licence	unicode	1EEC0DFF4EC642D83246EB0D24CD72F5	success or wait	1	40B747	RegSetValueExA

Disassembly

Code Analysis