ID: 356592
Sample Name:
SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.17259
Cookbook: default.jbs
Time: 11:50:46
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

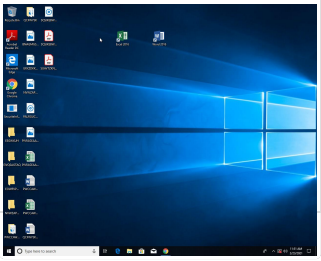
Analysis Report SecuriteInfo.com.Trojan.Win32.RL_And…

Overview

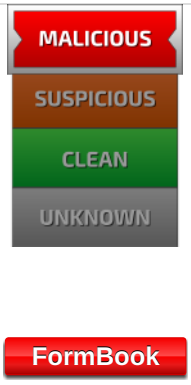
General Information

Sample Name:	SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.17259 (renamed file extension from 17259 to exe)
Analysis ID:	356592
MD5:	2915c0afb0b6b26…
SHA1:	32fdcc2e0bcfc47…
SHA256:	38b6a40d2eeddf3…

Most interesting Screenshot:



Detection



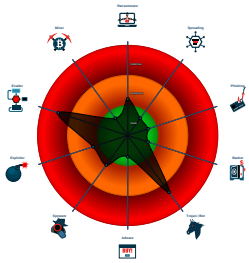
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Tries to detect virtualization through…
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe (PID: 6404 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe' MD5: 2915C0AFB0B6B26A5A699965D2119F7A)
  - SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe (PID: 6512 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe' MD5: 2915C0AFB0B6B26A5A699965D2119F7A)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.856380692.xyz/nsag/"
  ],
  "decoy": [
    "usopencoverage.com",
    "5bo5j.com",
    "deliveryourvote.com",
    "bestbuycarpethd.com",
    "worldsourcecloud.com",
    "glowtheblog.com",
    "translations.tools",
    "ithacapella.com",
    "machinerysubway.com",
    "aashlokhospitals.com",
    "athara-kiano.com",
    "anabittencourt.com",
    "hakimkhawatmi.com",
    "fashionwatchesstore.com",
    "krishnagiri.info",
    "tencenttexts.com",
    "kodairo.com",
    "ouitum.club",
    "robertbeauford.net",
    "polling.asia",
    "evoslancete.com",
    "4676sabalkey.com",
    "chechadskeitaro.com",
    "babyhopeful.com",
    "11376.xyz",
    "oryanomer.com",
    "jyxxfy.com",
    "scanourworld.com",
    "thevistadrinksco.com",
    "meow-cafe.com",
    "xfixpros.com",
    "botaniquecouture.com",
    "bkhlep.xyz",
    "mauriciozarate.com",
    "icepolo.com",
    "siyezim.com",
    "myfeezinc.com",
    "nooshone.com",
    "wholesalerbargains.com",
    "winabeel.com",
    "frankfrango.com",
    "patientsbooking.info",
    "ineedahealer.com",
    "thefamilyorchard.net",
    "clericallyco.com",
    "overseaexpert.com",
    "bukaino.net",
    "womens-secrets.love",
    "skinjunkie.site",
    "dccheavydutydiv.net",
    "explorerthecity.com",
    "droneserviceshouston.com",
    "creationsbyjamie.com",
    "profirma-nachfolge.com",
    "oasisbracelet.com",
    "maurobenetti.com",
    "mecs.club",
    "mistressofherdivinity.com",
    "vooronsland.com",
    "navia.world",
    "commagx4.info",
    "caresring.com",
    "yourstrivingforexcellence.com",
    "alpinevalleytimeshares.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000001.209279370.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000001.209279370.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000001.209279370.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.211005470.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.211005470.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 4 entries

Unpacked PEs

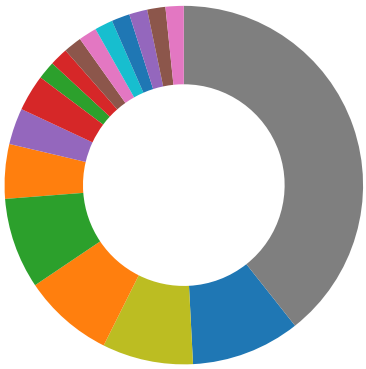
Source	Rule	Description	Author	Strings
3.1.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.1.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.1.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
3.2.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 13 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected FormBook

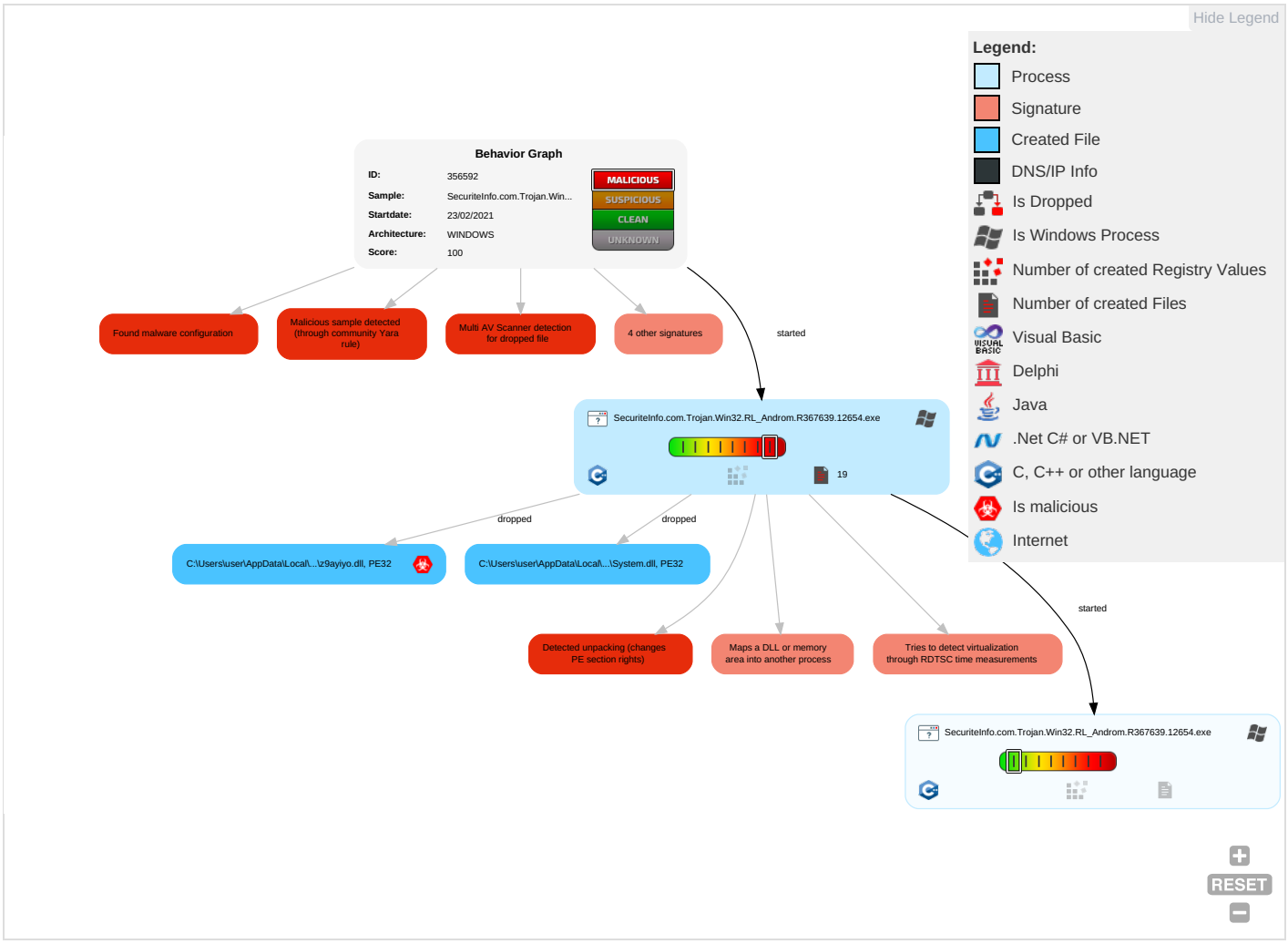
Remote Access Functionality:

Yara detected FormBook

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	Native API 1	Path Interception	Access Token Manipulation 1	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 2 3	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Access Token Manipulation 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 4	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or 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.Trojan.Win32.RL_Androm.R367639.12654.exe	39%	Virustotal		Browse
SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe	31%	ReversingLabs	Win32.Trojan.Generic	
SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	19%	ReversingLabs	Win32.Trojan.Convagent	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.2a50000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.1.SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.856380692.xyz/nsag/	0%	Virustotal		Browse
www.856380692.xyz/nsag/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.856380692.xyz/nsag/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356592
Start date:	23.02.2021
Start time:	11:50:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.17259 (renamed file extension from 17259 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:	6
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@3/4@0/0

EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.5% (good quality ratio 24.8%) • Quality average: 72.9% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 62% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	
	TIC ENQ2040 FCI.xlsx	Get hash	malicious	Browse	
	lpdKSOB78u.exe	Get hash	malicious	Browse	
	jTmBvrBw7V.exe	Get hash	malicious	Browse	
	523JHfbGM1.exe	Get hash	malicious	Browse	
	TAk8jeG5ob.exe	Get hash	malicious	Browse	
	PAYMENT COPY.exe	Get hash	malicious	Browse	
	ORDER LIST.xlsx	Get hash	malicious	Browse	
	Orderoffer.exe	Get hash	malicious	Browse	
	Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	
	INV_PR2201.docm	Get hash	malicious	Browse	
	CV-JOB REQUEST_____PDF.EXE	Get hash	malicious	Browse	
	Request for Quotation.exe	Get hash	malicious	Browse	
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	
	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	
	quote.exe	Get hash	malicious	Browse	
	Order83930.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	GPP.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsaBD31.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe
File Type:	data
Category:	dropped
Size (bytes):	191404
Entropy (8bit):	7.878606044995474
Encrypted:	false
SSDEEP:	3072:2ojw9jwLSvkpGlMfLPVlYB7kc8LvmDgJkIlSFmFp1Su/2PmLNxfYhAWXNt:2ogstrYBJ9Dy3SFSxuPmWrt
MD5:	4FECDED6A29355A90A3D3B3AABBB16E4
SHA1:	F0F16D89E8D1DD35F088CB49298DEA74A3FFF53B
SHA-256:	29680AD46B1D8A090A403798300D02897B547CF3F87FE44ADA08D95C7D34406B
SHA-512:	03889A1FA29D924FD5EB1C293A8D62FAF78876EC5CCF90F7602DC92302DB1D06BC162BDE097A66E9D148C90D0B7920E539CED3D0EF3A9AB4DD230AA73DE7E7D
Malicious:	false
Reputation:	low
Preview:	.....,.....$..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: QTN3C2AF414EDF9_041873.xlsx, Detection: malicious, Browse • Filename: TIC ENQ2040 FCl.xlsx, Detection: malicious, Browse • Filename: lpdKSOB78u.exe, Detection: malicious, Browse • Filename: jTmBvrBw7V.exe, Detection: malicious, Browse • Filename: 523JHfbGM1.exe, Detection: malicious, Browse • Filename: TAk8jeG5ob.exe, Detection: malicious, Browse • Filename: PAYMENT COPY.exe, Detection: malicious, Browse • Filename: ORDER LIST.xlsx, Detection: malicious, Browse • Filename: Orderoffer.exe, Detection: malicious, Browse • Filename: Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe, Detection: malicious, Browse • Filename: INV_PR2201.docm, Detection: malicious, Browse • Filename: CV-JOB REQUEST_____PDF.EXE, Detection: malicious, Browse • Filename: Request for Quotation.exe, Detection: malicious, Browse • Filename: #U007einvoice#U007eSC00978656.xlsx, Detection: malicious, Browse • Filename: Purchase Order___pdf _____.exe, Detection: malicious, Browse • Filename: quote.exe, Detection: malicious, Browse • Filename: Order83930.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: GPP.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tjqth.zz	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998867839876064**
Encrypted:	**true**
SSDEEP:	3072:ajw9jwLSvkpGlMfLPVlYB7kc8LvmDgJkIlSFmFp1Su/2PmLNxfYhAW2:agstrYBJ9Dy3SFSxuPmWo
MD5:	D0AA54167E81FD8C6C7CBC832E178855
SHA1:	7DEB6EB916CCDB8BDF62214F2F3026E9758CBCF6
SHA-256:	C8FD43535A87747A5046D1096717E18CE1E67D1B428498C072F011F3FA9A21E0
SHA-512:	380D39FA1D20BA78F13F91B3B5EA16B058BC864019C8608898941B723E9B04DFEAADDFAF041DC0D888388E056CA188978AEB3797A2C243313772AD83EB7FCFB 7
Malicious:	false
Reputation:	low
Preview:	.....Z...~....m...r...~.k.O...Sq....T.E..X.zT..y.*r.{.....s2=...t7^...a.?Gb.4k.).l4e.d.....X.?AO..*.[....].}....0.....j~v...Q.D!A.wA.....W.C..@{y...s.#z}.....\x..#4..i.=)dO.....#^$..s.. _..G{.....8s(...q[..>.D.\U..W....{....6s.?i.:?.{.f.(.|.....]..3...^(tS...+..o.N..Kn],.. %.`.....M^.CRlj3.{.[..i.\-.....l.....+.:YD.....v.c.~[.....~...z.F._a.i/.g\.uF.l..G.D=.....:..;...+.F..C...33.R3. [j=...%..G.a{P....KWu....L{...Zr.....6IE<..E&....H..j..;R.....K...^}.....CO..v...'ov!..f$j....A...Uh.y.....8'...$....'aSS.k57.(..}I...U.....wL. ...-;....A..qXZ....)*8x.V...1...s....PM.(&j.w.. a.R..Rx..<;e2.... .....K..V..c5.lD.eT.n../b..7P..S..I....K~.....K....I..._.p...;.H.1...4.4.!...6.....?.x...N.*.;.....8..;.Op.u..]...\..B..4J....`.t".BEm.`\..2....;..C.).uV7...m...c...x9W.m#..T.... @A2M..(..$S.....l$b.8.....4'#..OM.%...\..F.d...|..v.`../x.....#.3.I....1XB.[s..>..g.bz....c.Ax.l.q;O..'. P.n.y..0...c...w9..'\....".s.....1

C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	6.6898431043201
Encrypted:	false
SSDEEP:	96:NEBgIVyWyVDSLUpyceXGkLF6HSFLdtyfJHxPVAcnuvmMeT8XfWJ1QhulooeUZi+w:qBnADSLwgXG7yFDixPVmxP4QPCrvLs3
MD5:	94A51F0839DE3A6F5069F766E7BDE4A7
SHA1:	19454F40631ACE4B3DE692C245E3F2551A6794D6
SHA-256:	2D78C0015CEC67CD072ACFB337075825D4A6866D5FAC1B497A649DEB2190F42C
SHA-512:	07468053EFD63FC4B404D87722E0E282B1C5C487CF97E6D858771B67B2574C90D62341FD96D3CFB94ACA6ED357E40657842ADD01E7C563AE170A65450A4EB75
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 19%
Joe Sandbox View:	• Filename: QTN3C2AF414EDF9_041873.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.N.e.N.e.N.e.N.e.NI..N.e.N..cN.e.N..gN.e.N..dN.e.N..aN.e .NRich.e.N.....PE..L...F.4`.....!.....&..... .....p.....@.....P$..I.... .....P.....`..d..... .....code..... ....rdata..... .....@..@.data.....0.....@....rsrc.....P.....*.....@..@.reloc.....`.....,.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.895818449493941
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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.Trojan.Win32.RL_Androm.R367639.12654.exe
File size:	217624

General

MD5:	2915c0afb0b6b26a5a699965d2119f7a
SHA1:	32fdcc2e0bcfc476347078d7ea05f12d5a259bea
SHA256:	38b6a40d2eeddf38695294c57971fc2efab81fea95100260a2003baa13616b83
SHA512:	b8312043058b28c0eede079425d785b581aabeae63c889ddc4382faa2b070333fc8a6e76f7810678cb9ae96b9e52d6e48604cef9417c565c97c0faadfe36b953
SSDEEP:	6144:611QTAGoul3imDxtHYB19DyzSFSxuPmxF0y:xAjul3i+xlK19JGuOUy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..._.$_.....f...x.....4.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403486
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D75F [Sat Aug 1 02:45:51 2020 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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F44Ch], eax
je 00007FBF008665B3h
push ebx
call 00007FBF0086972Eh
cmp eax, ebx
je 00007FBF008665A9h

Instruction
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007FBF008696AAh
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FBF0086658Dh
push 0000000Bh
call 00007FBF00869702h
push 00000009h
call 00007FBF008696FBh
push 00000007h
mov dword ptr [0042F444h], eax
call 00007FBF008696EFh
cmp eax, ebx
je 00007FBF008665B1h
push 0000001Eh
call eax
test eax, eax
je 00007FBF008665A9h
or byte ptr [0042F44Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F518h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429878h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x97c	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
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	0x65ad	0x6600	False	0.675628063725	data	6.48593060343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4634765625	data	5.26110074066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25558	0x600	False	0.470052083333	data	4.21916068772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x97c	0xa00	False	0.453515625	data	4.29529055645	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x38148	0x100	data	English	United States
RT_DIALOG	0x38248	0x11c	data	English	United States
RT_DIALOG	0x38364	0x60	data	English	United States
RT_VERSION	0x383c4	0x278	data	English	United States
RT_MANIFEST	0x3863c	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Version Infos

Description	Data
LegalCopyright	Copyright fuel-air explosive
FileVersion	69.46.40.87
CompanyName	arithmetic
LegalTrademarks	stack
Comments	Done-S
ProductName	dehumidify
FileDescription	entail
Translation	0x0409 0x04e4

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

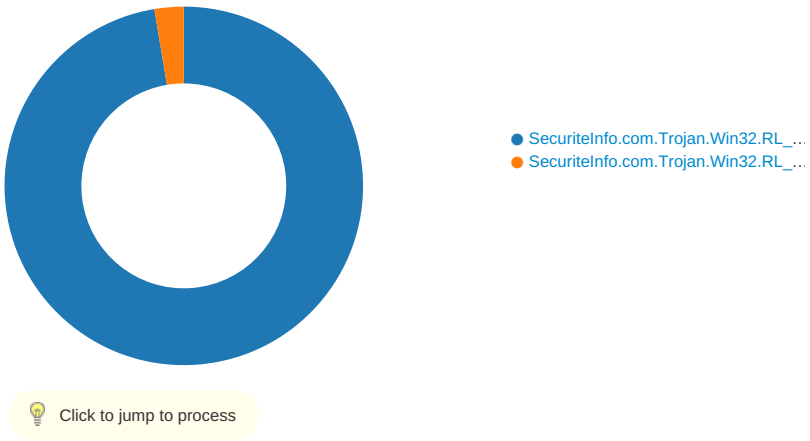
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe
PID: 6404 Parent PID: 5664

General

Start time:	11:51:33
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe'
Imagebase:	0x400000
File size:	217624 bytes
MD5 hash:	2915C0AFB0B6B26A5A699965D2119F7A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.211020267.0000000002A50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.211020267.0000000002A50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.211020267.0000000002A50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsaBD30.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsaBD31.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
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	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
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	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\tjqth.zz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA

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	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
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	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405883	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaBD30.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaBD31.tmp	unknown	22150	9c 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 d6 0c 00 00 01 00 00 00 9c 0d 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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 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	........,...................$.	success or wait	12	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\z9ayiyo.dll	unknown	11776	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 d8 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 f1 04 c3 1d b5 65 ad 4e b5 65 ad 4e b5 65 ad 4e b5 65 ac 4e 9f 65 ad 4e 49 12 14 4e ba 65 ad 4e 92 a3 63 4e b4 65 ad 4e 92 a3 67 4e b4 65 ad 4e 92 a3 64 4e b4 65 ad 4e 92 a3 61 4e b4 65 ad 4e 52 69 63 68 b5 65 ad 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 46 b4 34 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 26 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............e.N.e.N.e.N.e.N.e .NI..N.e.N..cN.e.N..gN.e.N. .dN .e.N..aN.e.NRich.e.N......... .......PE..L...F.4`...........! ....&.....	success or wait	1	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\tjqth.zz	unknown	16384	9c bf f3 1b bc fa c8 5a c1 e0 91 7e 04 07 7f e0 a2 6d 8f 0a 10 72 e1 f0 14 7e b5 6b e9 4f 89 f1 eb 53 71 0d a2 d1 80 9c 54 10 45 88 ce 58 b6 7a 54 18 c0 79 b1 2a 72 92 7b b4 18 b5 bc 81 73 32 3d ea 16 a8 74 37 5e 8b 93 f9 61 9a 3f 47 62 00 34 6b c6 86 29 c9 a0 6c 34 65 e9 64 de ec 2e e1 db ce 95 db b1 ae d1 58 93 3f 41 4f a8 d7 2a d5 5b b2 d8 b4 05 cb 5d 0b 7d c7 86 b1 e5 85 e1 86 30 bc 10 0b af ad 9c 87 e4 dd f4 8a 6a 7e 76 f9 81 90 51 8f 44 21 41 c3 8d 77 41 ff f5 9d 9b 8c c8 57 db 43 1a 1f 40 7b 79 f7 9f fc 73 8d 23 7a 7d e9 7f fc c1 e8 0b e2 5c 78 cf f3 23 34 18 d3 69 9a 3d 29 64 4f a0 1b d0 e7 df ff 23 5e 24 e0 d8 73 ba c0 5f f7 96 47 7b 93 b5 17 90 dc 38 73 28 d7 e2 a7 89 fe 71 5b cb ce b3 3e a5 44 ad 5c 55 f4 a2 57 fd f3 03 e4 7b 0d cb 0e b5 36 73	.......Z...~.....m...r...~.k.O ...Sq.....T.E..X.zT..y.*r.{... ..s2=...t7^...a.?Gb.4k..)..l4e .d...........X.?AO..*.[.....]. }.......0...........j~v...Q.D! A..wA......W.C..@{y...s.#z}. ......\x..#4..i.=)dO......#^$..s .._..G{.....8s(.....q[...>.D.\ U..W....{....6s	success or wait	11	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaBD32.tmp\System.dll	unknown	11776	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 d0 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 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe	unknown	512	success or wait	72	405E78	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe	unknown	16384	success or wait	12	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsaBD31.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsaBD31.tmp	unknown	3484	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsaBD31.tmp	unknown	4	success or wait	3	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\tjqth.zz	unknown	164352	success or wait	1	7378450C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73783867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73783867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73783867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73783867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73783867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73783867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73783867	ReadFile

Analysis Process: SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe PID: 6512 Parent PID: 6404

General

Start time:	11:51:34
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.RL_Androm.R367639.12654.exe'
Imagebase:	0x400000
File size:	217624 bytes
MD5 hash:	2915C0AFB0B6B26A5A699965D2119F7A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.209279370.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.209279370.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.209279370.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.211005470.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.211005470.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.211005470.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Disassembly

Code Analysis