ID: 635348
Sample Name:
SecuriteInfo.com.W32.AIDetectNet.01.24194.12957
Cookbook: default.jbs
Time: 19:41:51
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

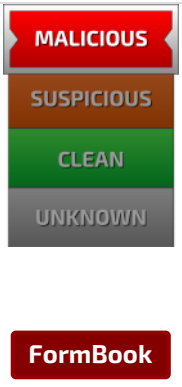
SecuriteInfo.com.W32.AIDetectNet.01.24194.12957

Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetectNet.01.24194.12957 (renamed file extension from 12957 to exe)
Analysis ID:	635348
MD5:	ac85e260ef18ab..
SHA1:	1137e2caa9848d..
SHA256:	0e3a4f080d2ff0b..
Tags:	exe
Infos:	

Detection



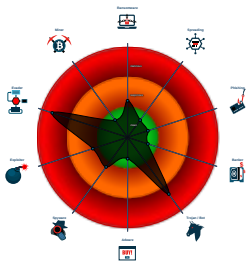
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- .NET source code contains method …
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetectNet.01.24194.exe (PID: 3920 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe" MD5: AC85E260EF18AB08B53E04177E8C04A9)
  - SecuriteInfo.com.W32.AIDetectNet.01.24194.exe (PID: 3364 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe MD5: AC85E260EF18AB08B53E04177E8C04A9)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.commwealth-cba-au.com/smwr/"
  ],
  "decoy": [
    "forex.exposed",
    "benditabrujaastrologia.com",
    "savannah-e.com",
    "cssdwljx.com",
    "floridayachtparty.com",
    "koru-purple.com",
    "caddyscholarship.com",
    "mywinningkidssedallas.com",
    "operati.club",
    "kinvuehealth.biz",
    "littlebearbicycleoutfitters.com",
    "btcfarsi.com",
    "poppyteez.com",
    "roninwallettsmoney.com",
    "greedyp.one",
    "kangshifuqwdz.com",
    "osamirin.xyz",
    "leaddoggq.com",
    "cherrypickmerch.com",
    "myqmetrbs.com",
    "melonslot.info",
    "mommyheartstacos.com",
    "samcsu.xyz",
    "702slingshots.com",
    "gnw8.com",
    "officegame.xyz",
    "lalunamesa.com",
    "alignedtalent.tech",
    "djzemi.com",
    "anti-tracker-test.com",
    "estilobank.com",
    "n4q7.com",
    "404035.com",
    "relaxtionary.com",
    "beastmodewellness.com",
    "lskdojfjf3k35.com",
    "mtyapialanya.com",
    "giftcardpulse.com",
    "yy6333.com",
    "sdcychemical.com",
    "icarusexchange.info",
    "elementsfunding.com",
    "199yb.com",
    "beladicaseofertas.site",
    "bi11111.com",
    "esystemhr.com",
    "tsharedrop.com",
    "sattlerplastics.site",
    "walgreensrabenefit.com",
    "spatula11.com",
    "sunriseteam.info",
    "stephensonequipinc.com",
    "fashionsbyfleur.com",
    "aiscrofa.com",
    "shopmeccamarket.com",
    "physicistlakefront.com",
    "ivermectinsales.com",
    "perceptiv.academy",
    "davidgilbertcarpentryplus.com",
    "wynn12.com",
    "medicalofficeinsurance.online",
    "womenofwildpodcast.com",
    "neoneuphoria.com",
    "thedevonlabellady.online"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.303867401.0000000003C01000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.303867401.0000000003C01000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x11538:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x118d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x3c358:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x3c6f2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x66178:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x66512:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1ec75:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x49a95:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x738b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1e721:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x49541:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x73361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1ed77:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x49b97:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x739b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1eeef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x49d0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x73b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x122ea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x3d10a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x66f2a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06
00000000.00000002.303867401.0000000003C01000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x21149:$sqlite3step: 68 34 1C 7B E1 • 0x2125c:$sqlite3step: 68 34 1C 7B E1 • 0x4bf69:$sqlite3step: 68 34 1C 7B E1 • 0x4c07c:$sqlite3step: 68 34 1C 7B E1 • 0x75d89:$sqlite3step: 68 34 1C 7B E1 • 0x75e9c:$sqlite3step: 68 34 1C 7B E1 • 0x21178:$sqlite3text: 68 38 2A 90 C5 • 0x2129d:$sqlite3text: 68 38 2A 90 C5 • 0x4bf98:$sqlite3text: 68 38 2A 90 C5 • 0x4c0bd:$sqlite3text: 68 38 2A 90 C5 • 0x75db8:$sqlite3text: 68 38 2A 90 C5 • 0x75edd:$sqlite3text: 68 38 2A 90 C5 • 0x2118b:$sqlite3blob: 68 53 D8 7F 8C • 0x212b3:$sqlite3blob: 68 53 D8 7F 8C • 0x4bfab:$sqlite3blob: 68 53 D8 7F 8C • 0x4c0d3:$sqlite3blob: 68 53 D8 7F 8C • 0x75dcb:$sqlite3blob: 68 53 D8 7F 8C • 0x75ef3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000000.298671862.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000000.298671862.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
10.2.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$sqlite3step: 68 34 1C 7B E1 • 0x1892c:$sqlite3step: 68 34 1C 7B E1 • 0x18848:$sqlite3text: 68 38 2A 90 C5 • 0x1896d:$sqlite3text: 68 38 2A 90 C5 • 0x1885b:$sqlite3blob: 68 53 D8 7F 8C • 0x18983:$sqlite3blob: 68 53 D8 7F 8C
10.2.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 21 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

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

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

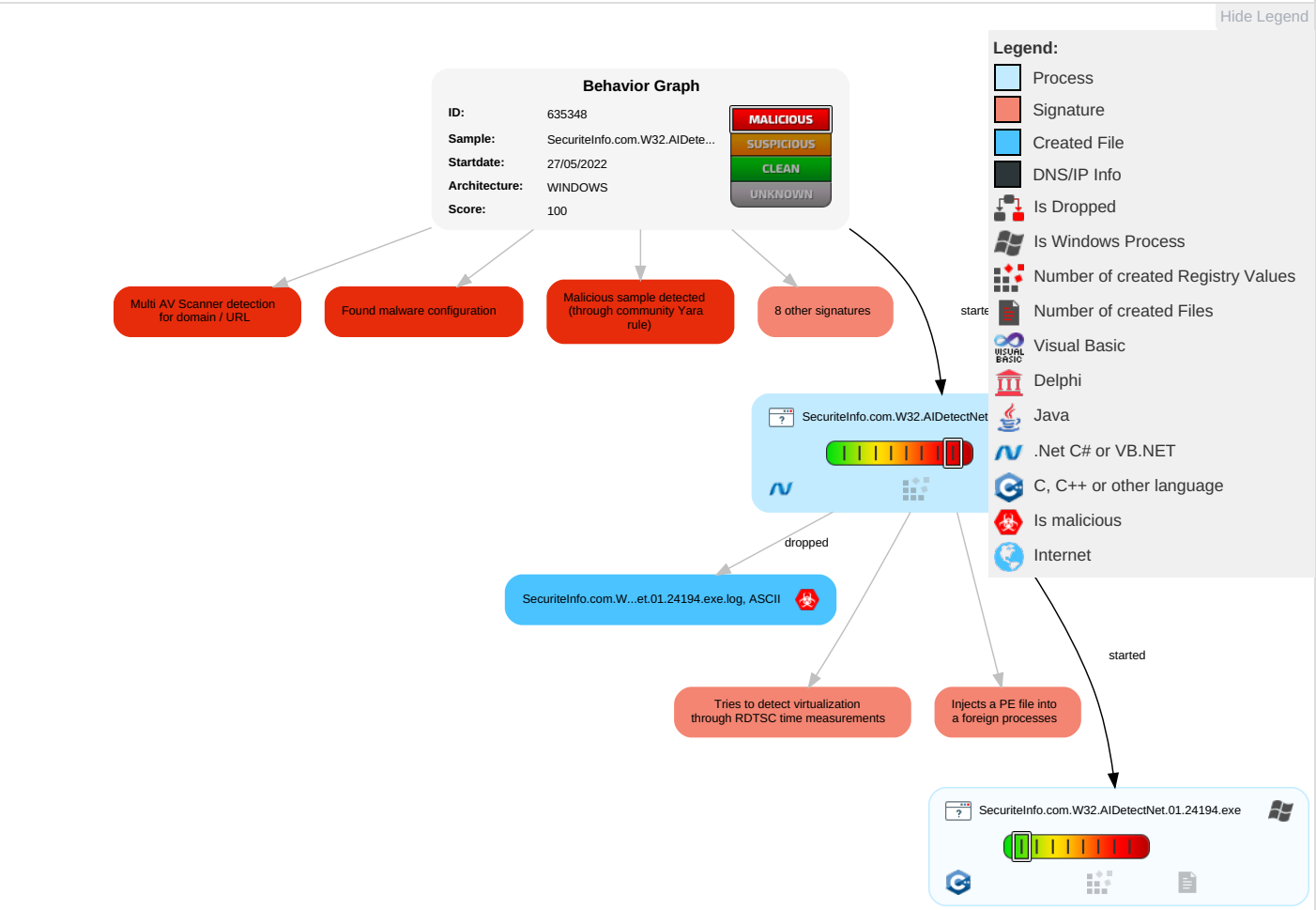
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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.W32.AIDetectNet.01.24194.exe	31%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetectNet.01.24194.exe	27%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
SecuriteInfo.com.W32.AIDetectNet.01.24194.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.0.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.0.SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comueTF	0%	URL Reputation	safe	
http://www.fontbureau.comuemQ	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn7R	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
www.commwealth-cba-au.com/smwr/	7%	Virustotal		Browse
www.commwealth-cba-au.com/smwr/	100%	Avira URL Cloud	phishing	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-u	0%	URL Reputation	safe	
http://www.fontbureau.comsiefRPho	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-e	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.commwealth-cba-au.com/smwr/	true	• 7%, Virustotal, Browse • Avira URL Cloud: phishing	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.299899600.0000000005C6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers~	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.270438377.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersE	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269072747.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269013352.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269126032.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269174089.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comueTF	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.271142884.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comuemQ	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.306903174.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.299986023.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.278971595.0000000005C6D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.276139218.0000000005C66000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.284163429.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.276289023.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.299899600.0000000005C60000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn7R	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.262954837.0000000005C6400.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.263269492.0000000005C67000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.263072140.0000000005C66000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.263158470.0000000005C67000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.263201849.0000000005C67000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.262993160.0000000005C64000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.268320197.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.276029305.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.266179512.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.266268752.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.306903174.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.299986023.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.278971595.0000000005C6D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.276139218.0000000005C66000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.284163429.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.276289023.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.299899600.0000000005C60000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersl#	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269675889.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269723077.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.262954837.0000000005C64000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-user.htmlX4	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269530321.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers_	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.276091209.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.276029305.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.266268752.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.266482682.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n-u	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.266179512.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.266268752.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsiefRPho	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.271142884.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.271142884.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F5200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F5200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F5200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F5200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F5200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersz	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269072747.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269013352.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269126032.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.268902046.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.269174089.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F5200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000002.307326512.0000000006F5200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.271142884.0000000005C6C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.268320197.0000000005C9D000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnu-e	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.262954837.0000000005C6400 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.263269492.0000000005C 67000.00000004.00000800.00020000.0000000 0.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24194. exe, 00000000.00000003.263072140.0000000 005C66000.00000004.00000800.00020000.000 00000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.24 194.exe, 00000000.00000003.263158470.000 0000005C67000.00000004.00000800.00020000 .00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.0 1.24194.exe, 00000000.00000003.263201849 .0000000005C67000.00000004.00000800.0002 0000.00000000.sdmp, SecuriteInfo.com.W32 .AIDetectNet.01.24194.exe, 00000000.0000 0003.262993160.0000000005C64000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsd	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe, 00000000.00000003.271142884.0000000005C6C00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635348
Start date and time: 27/05/202219:41:51	2022-05-27 19:41:51 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetectNet.01.24194.12957 (renamed file extension from 12957 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.8% (good quality ratio 23.5%) • Quality average: 70.6% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com

- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:43:20	API Interceptor	1x Sleep call for process: SecuriteInfo.com.W32.AIDetectNet.01.24194.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.742642857816063
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.W32.AIDetectNet.01.24194.exe
File size:	779776
MD5:	ac85e260ef18ab08b53e04177e8c04a9
SHA1:	1137e2caa9848d3b804fecb01e12624bd5fb62bc
SHA256:	0e3a4f080d2ff0bdfa0a7e39df4982232b2d19245e6355e49940c05becfeecc5
SHA512:	0311f7aa0c464d0d82b14f56fb116d61414be43621bcb84072795a0760ecb36ecdeacfc4d98444cbf1716caac16a045f0b34aad994ca3bbd02fa9a34ca2e7652
SSDEEP:	12288:Moa7mYn3GNG2p0I8WRnyGTd+p2YH0UUO4NQ4mYvZ0obd:Mf7mYWNG80I8W5yGTwp25UUO4C4mYxjd
TLSH:	D7F4E06A76679E03C11823B480C2E41407F96107A573E3C76FC761D72B1ABE59EC9B8B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....Z..... .....@.. .....@.....@.....

File Icon

Icon Hash:	4462f276dcec30e6

Static PE Info

General

Entrypoint:	0x4ba9be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6290E388 [Fri May 27 14:43:20 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xba970	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x57c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xba923	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb89c4	0xb8a00	False	0.881581383294	data	7.74063196542	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x57c0	0x5800	False	0.964621803977	data	7.89130545967	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbc130	0x51a3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xc12d4	0x14	data		
RT_VERSION	0xc12e8	0x2ec	data		
RT_MANIFEST	0xc15d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

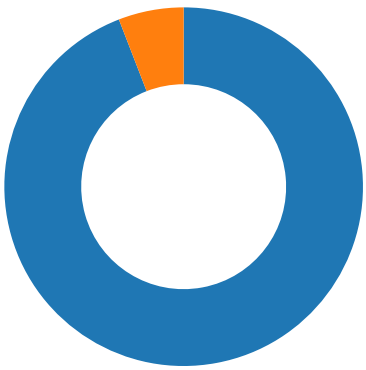
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	IServiceProvi.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	IServiceProvi.exe

Network Behavior

No network behavior found

Statistics

Behavior



SecuriteInfo.com.W32.AIDetectNet…
SecuriteInfo.com.W32.AIDetectNet…

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.24194.exe PID: 3920, Parent PID: 5880

General

Target ID:	0
Start time:	19:43:01
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe"
Imagebase:	0x700000
File size:	779776 bytes
MD5 hash:	AC85E260EF18AB08B53E04177E8C04A9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.303867401.0000000003C01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.303867401.0000000003C01000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.303867401.0000000003C01000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.307980794.0000000007640000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.302533701.0000000002C6D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.302576696.0000000002C92000.00000004.00000800.00020000.00000000.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	6DCACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFBC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DFBC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.24194.exe PID: **3364**, Parent PID: **3920**

General

Target ID:	10
Start time:	19:43:23
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.24194.exe
Imagebase:	0xac0000
File size:	779776 bytes
MD5 hash:	AC85E260EF18AB08B53E04177E8C04A9
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: 0000000A.00000000.298671862.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.298671862.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.298671862.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.301741278.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.301741278.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.301741278.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.298185679.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.298185679.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.298185679.0000000000400000.00000040.00000400.00020000.00000000.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	41A417	NtReadFile

Disassembly

No disassembly