
**ID:** 537823
**Sample Name:**
SecuriteInfo.com.Trojan.AutoIt.316.10986.27538
**Cookbook:** default.jbs
**Time:** 14:14:52
**Date:** 10/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

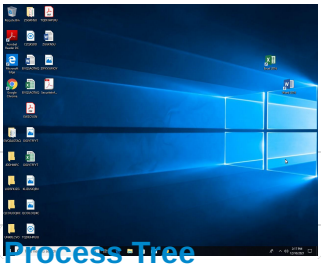
# Windows Analysis Report SecuriteInfo.com.Trojan.Auto…

## Overview

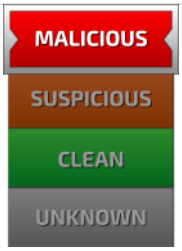
### General Information

| | |
|---|---|
| Sample Name: | SecuriteInfo.com.Trojan.AutoIt.316.10986.27538 (renamed file extension from 27538 to exe) |
| Analysis ID: | 537823 |
| MD5: | 52d4245d65d5cc.. |
| SHA1: | b2ecf335eb93feb.. |
| SHA256: | 70ef3c88a90dd59. |
| Tags: | exe HawkEye |
| Infos: | |

Most interesting Screenshot:



### Detection



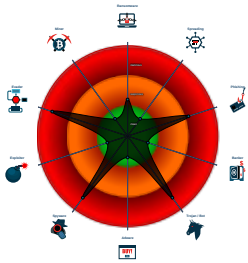

HawkEye
MailPassView

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

### Signatures

- Yara detected MailPassView
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Multi AV Scanner detection for doma…
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- .NET source code references suspic…

### Classification



## Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.AutoIt.316.10986.exe (PID: 4720 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.AutoIt.316.10986.exe" MD5: 52D4245D65D5CC2DA05298C480FFCC5F)
  - RegAsm.exe (PID: 5908 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - vbc.exe (PID: 4484 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmpBCAF.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 5964 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmpBBC1.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000013.00000000.401565016.000000000400000.00000040.00000001.sdmp | APT_NK_BabyShark_KimJoingRAT_Apr19_1 | Detects BabyShark KimJongRAT | Florian Roth | • 0x147b0:$a1: logins.json<br>• 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login<br>• 0x14f34:$s4: \mozsqlite3.dll<br>• 0x137a4:$s5: SMTP Password |
| 00000013.00000000.401565016.000000000400000.00000040.00000001.sdmp | JoeSecurity_MailPassView | Yara detected MailPassView | Joe Security | |
| 00000000.00000003.248337037.0000000000FF0000.00000004.00000001.sdmp | MAL_HawkEye_Keylogger_Gen_Dec18 | Detects HawkEye Keylogger Reborn | Florian Roth | • 0x87c4e:$s1: HawkEye Keylogger<br>• 0x87cb7:$s1: HawkEye Keylogger<br>• 0x81091:$s2: _ScreenshotLogger<br>• 0x8105e:$s3: _PasswordStealer |
| 00000000.00000003.248337037.0000000000FF0000.00000004.00000001.sdmp | JoeSecurity_HawkEye | Yara detected HawkEye Keylogger | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000013.00000000.401266886.000000000400000.00000040.00000001.sdmp | APT_NK_BabyShark_KimJoingRAT_Apr19_1 | Detects BabyShark KimJongRAT | Florian Roth | • 0x147b0:$a1: logins.json<br>• 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login<br>• 0x14f34:$s4: \mozsqlite3.dll<br>• 0x137a4:$s5: SMTP Password |
| Click to see the 40 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 19.0.vbc.exe.400000.4.unpack | APT_NK_BabyShark_KimJoingRAT_Apr19_1 | Detects BabyShark KimJongRAT | Florian Roth | • 0x131b0:$a1: logins.json<br>• 0x13110:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login<br>• 0x13934:$s4: \mozsqlite3.dll<br>• 0x121a4:$s5: SMTP Password |
| 19.0.vbc.exe.400000.4.unpack | JoeSecurity_MailPassView | Yara detected MailPassView | Joe Security | |
| 1.3.RegAsm.exe.4a9b8f2.0.unpack | APT_NK_BabyShark_KimJoingRAT_Apr19_1 | Detects BabyShark KimJongRAT | Florian Roth | • 0x11bb0:$a1: logins.json<br>• 0x11b10:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login<br>• 0x12334:$s4: \mozsqlite3.dll<br>• 0x115a4:$s5: SMTP Password |
| 1.3.RegAsm.exe.4a9b8f2.0.unpack | JoeSecurity_MailPassView | Yara detected MailPassView | Joe Security | |
| 19.0.vbc.exe.400000.3.raw.unpack | APT_NK_BabyShark_KimJoingRAT_Apr19_1 | Detects BabyShark KimJongRAT | Florian Roth | • 0x147b0:$a1: logins.json<br>• 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login<br>• 0x14f34:$s4: \mozsqlite3.dll<br>• 0x137a4:$s5: SMTP Password |
| Click to see the 83 entries | | | | |

# Sigma Overview

## System Summary:

**Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments**

**Sigma detected: Possible Applocker Bypass**

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

**Multi AV Scanner detection for submitted file**

**Antivirus / Scanner detection for submitted sample**

**Multi AV Scanner detection for domain / URL**

## Key, Mouse, Clipboard, Microphone and Screen Capturing:

**Yara detected HawkEye Keylogger**

## System Summary:

**Malicious sample detected (through community Yara rule)**

**Binary is likely a compiled AutoIt script file**

Autolt script contains suspicious strings

## Malware Analysis System Evasion:

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

## HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

## Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

Tries to steal Mail credentials (via file / registry access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Tries to steal Instant Messenger accounts or passwords

Tries to harvest and steal browser information (history, passwords, etc)

## Remote Access Functionality:

Yara detected HawkEye Keylogger

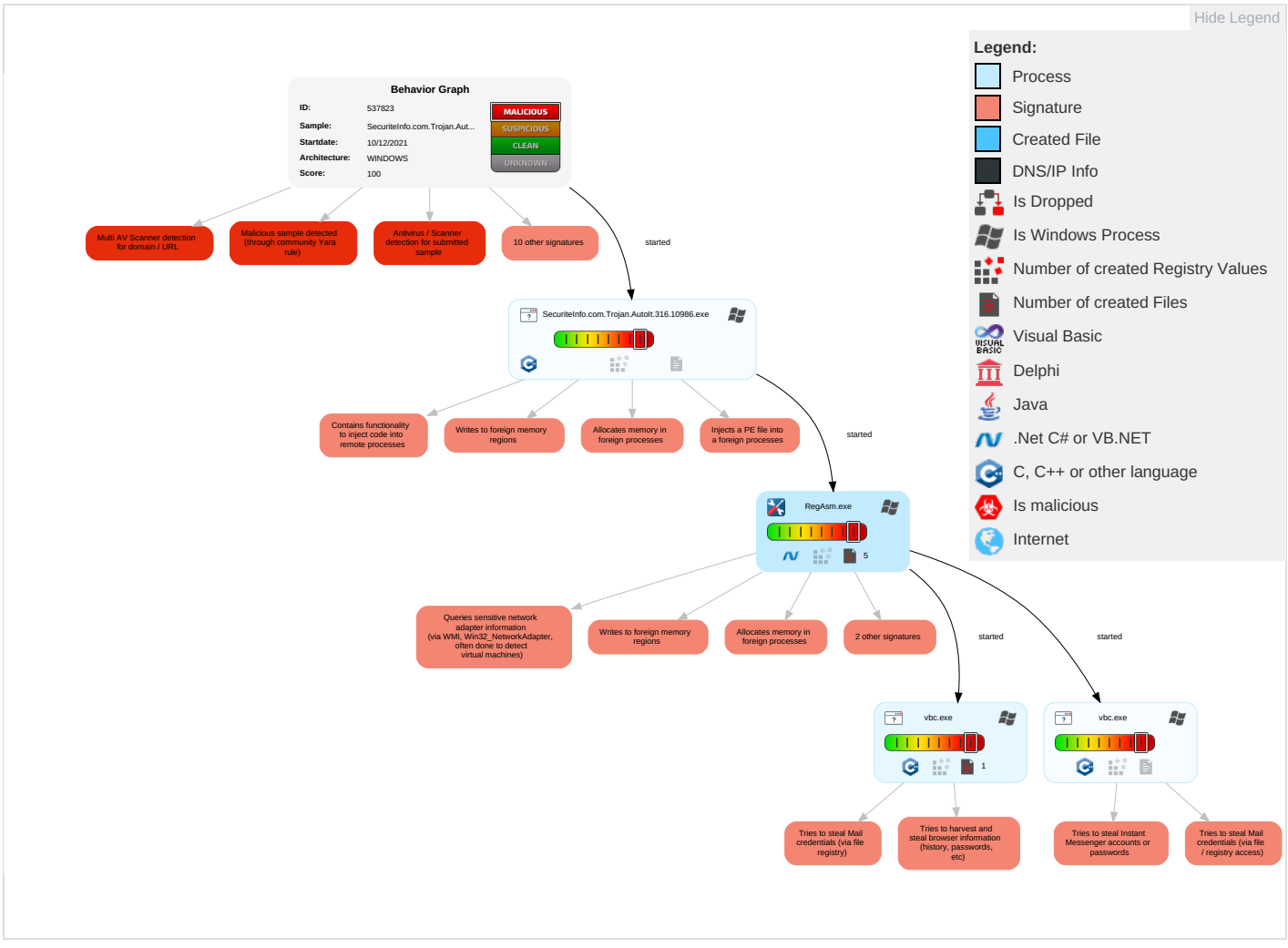
Detected HawkEye Rat

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Cont |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 1 1 1 | DLL Side-Loading 1 | DLL Side-Loading 1 | Disable or Modify Tools 1 | OS Credential Dumping 1 | System Time Discovery 1 | Remote Services | Archive Collected Data 1 1 | Exfiltration Over Other Network Medium | Encrypted Channel |
| Default Accounts | Native API 1 1 | Application Shimming 1 | Application Shimming 1 | Deobfuscate/Decode Files or Information 1 1 | Input Capture 2 1 | Account Discovery 1 | Remote Desktop Protocol | Data from Local System 1 | Exfiltration Over Bluetooth | Remote A Software |
| Domain Accounts | Shared Modules 1 | Logon Script (Windows) | Process Injection 5 1 2 | Obfuscated Files or Information 2 | Credentials in Registry 2 | File and Directory Discovery 1 | SMB/Windows Admin Shares | Email Collection 1 | Automated Exfiltration | Steganog |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Software Packing 1 | Credentials In Files 1 | System Information Discovery 9 | Distributed Component Object Model | Input Capture 2 1 | Scheduled Transfer | Protocol Impersona |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | DLL Side-Loading 1 | LSA Secrets | Security Software Discovery 2 4 | SSH | Clipboard Data 1 | Data Transfer Size Limits | Fallback Channels |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Virtualization/Sandbox Evasion 1 2 | Cached Domain Credentials | Virtualization/Sandbox Evasion 1 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communi |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Comman and Cont |
|---|---|---|---|---|---|---|---|---|---|---|
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Process Injection 5 1 2 | DCSync | Process Discovery 4 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonl Used Port |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Indicator Removal from Tools | Proc Filesystem | Application Window Discovery 1 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Applicatio Layer Pro |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Masquerading | /etc/passwd and /etc/shadow | System Owner/User Discovery 1 | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Prot |

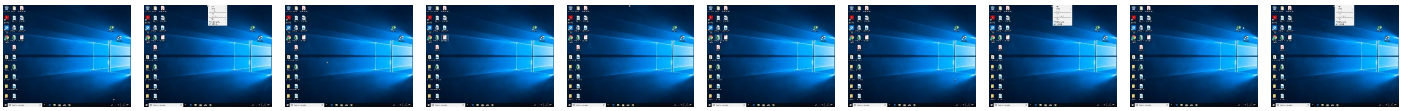
## Behavior Graph

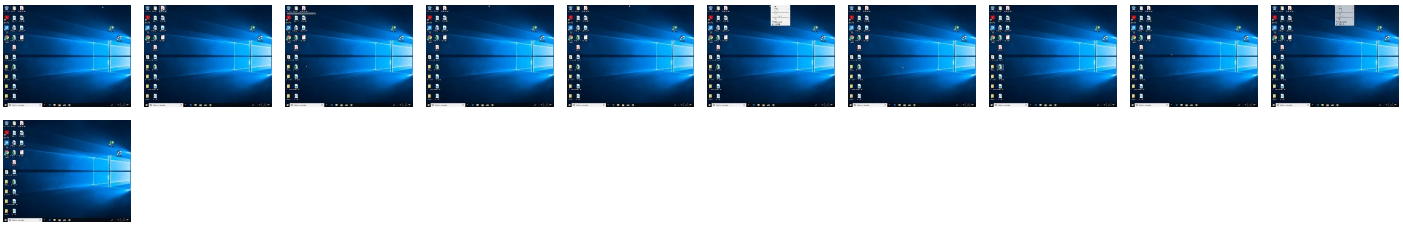



## Screenshots

### 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.AutoIt.316.10986.exe | 70% | Virustotal | | Browse |
| SecuriteInfo.com.Trojan.AutoIt.316.10986.exe | 78% | ReversingLabs | Win32.Trojan.Generic | |
| SecuriteInfo.com.Trojan.AutoIt.316.10986.exe | 100% | Avira | HEUR/AGEN.1100066 | |

### Dropped Files

**No Antivirus matches**

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 3.0.vbc.exe.400000.3.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 3.2.vbc.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |
| 1.0.RegAsm.exe.400000.0.unpack | 100% | Avira | TR/Dropper.Gen | | Download File |
| 1.2.RegAsm.exe.400000.0.unpack | 100% | Avira | TR/Dropper.Gen | | Download File |
| 0.3.SecuriteInfo.com.Trojan.AutoIt.316.10986.exe.ff0000.0.unpack | 100% | Avira | TR/Dropper.Gen | | Download File |
| 3.0.vbc.exe.400000.5.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |
| 0.0.SecuriteInfo.com.Trojan.AutoIt.316.10986.exe.d00000.0.unpack | 100% | Avira | HEUR/AGEN.1100066 | | Download File |
| 0.2.SecuriteInfo.com.Trojan.AutoIt.316.10986.exe.d00000.0.unpack | 100% | Avira | HEUR/AGEN.1100066 | | Download File |
| 3.0.vbc.exe.400000.2.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |
| 3.0.vbc.exe.400000.4.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |
| 3.0.vbc.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |
| 1.0.RegAsm.exe.400000.1.unpack | 100% | Avira | TR/Dropper.Gen | | Download File |
| 3.0.vbc.exe.400000.1.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |

### Domains

**No Antivirus matches**

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://deff.nelreports.net/api/report?cat=msn | 0% | URL Reputation | safe | |
| http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js | 0% | URL Reputation | safe | |
| http://https://a.pomf.cat/ | 8% | Virustotal | | Browse |
| http://https://a.pomf.cat/ | 0% | Avira URL Cloud | safe | |
| http://crl.pki.goog/GTS1O1core.crl0 | 0% | URL Reputation | safe | |
| http://images.outbrainimg.com/transform/v3/eyJpdSI6IjE4MmE0M2M0MDY3OGU1N2E4MjhkM2NjNDdlNGMzZmNkYjU1N | 0% | Avira URL Cloud | safe | |
| http://images.outbrainimg.com/transform/v3/eyJpdSI6ImY3MDA1MDJkMTdmZDY0M2VkZTBjNzg5MTE1OWEyYTYxMWRiN | 0% | Avira URL Cloud | safe | |
| http://pki.goog/gsr2/GTS1O1.crt0 | 0% | URL Reputation | safe | |
| http://https://pki.goog/repository/0 | 0% | URL Reputation | safe | |
| http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1 | 0% | URL Reputation | safe | |
| http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js | 0% | URL Reputation | safe | |
| http://crl.pki.goog/gsr2/gsr2.crl0? | 0% | URL Reputation | safe | |
| http://pki.goog/gsr2/GTSGIAG3.crt0) | 0% | URL Reputation | safe | |
| http://pki.goog/gsr2/GTS1O1.crt0# | 0% | URL Reputation | safe | |
| http://pomf.cat/upload.php&https://a.pomf.cat/ | 0% | Avira URL Cloud | safe | |
| http://https://aefd.nelreports.net/api/report?cat=bingth | 0% | URL Reputation | safe | |
| http://images.outbrainimg.com/transform/v3/eyJpdSI6IiIsIml1ZSI6Imh0dHA6Ly9pbWFnZXMyLnplbWFudGEuY29tL | 0% | URL Reputation | safe | |
| http://pomf.cat/upload.php | 0% | Avira URL Cloud | safe | |
| http://crl.pki.goog/GTSGIAG3.crl0 | 0% | URL Reputation | safe | |
| http://https://logincdn.msauth.net/16.000.28230.00/MeControl.js | 0% | URL Reputation | safe | |
| http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gt | 0% | URL Reputation | safe | |

## Domains and IPs

### Contacted Domains

**No contacted domains info**

### URLs from Memory and Binaries

### Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 537823 |
| Start date: | 10.12.2021 |
| Start time: | 14:14:52 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 10m 18s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SecuriteInfo.com.Trojan.AutoIt.316.10986.27538 (renamed file extension from 27538 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: | 26 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.phis.troj.spyw.evad.winEXE@7/3@0/0 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 39.4% (good quality ratio 38.3%)<br>• Quality average: 85.8%<br>• Quality standard deviation: 22.9% |
| HCA Information: | • Successful, ratio: 58%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 14:15:55 | API Interceptor | 1x Sleep call for process: RegAsm.exe modified |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Temp\78ede25b-fb90-6791-1ca9-e1fd644b6d85 | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 88 |
| Entropy (8bit): | 5.490292840056112 |
| Encrypted: | false |
| SSDEEP: | 3:PFYyImXF9mN2RVQON4NgCkCAUdXM:PHRB6+C3xy |
| MD5: | 454353131947D1483FF5470107478978 |
| SHA1: | C559163C23E5F878BE85D05F3EDEEAA620173C3D |
| SHA-256: | 2DF94DC1C58E952A1EBD1AE1185A291A8A573982CA90EC1BBB87B81126002668 |
| SHA-512: | C8912DA4654C735F7618B0ABEA7EC0197B17E6E072718B825B5799B2E88CC0E8AE8245CA95E1E5955C3AB8F649CA4ED6529975B142B061ECC402D935401B84DE |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | LeNF7Goy7uuKWKsmWAhDmhEi2BbZGy27JQQaO8wc/LiRcthbCBcu+4Nt6yYR3dz6dYTg/ZHS1axBPoq2xePo2w== |

| C:\Users\user\AppData\Local\Temp\bhv4453.tmp | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe |
| File Type: | Extensible storage engine DataBase, version 0x620, checksum 0x7ce4008c, page size 32768, DirtyShutdown, Windows version 10.0 |
| Category: | dropped |
| Size (bytes): | 26738688 |
| Entropy (8bit): | 0.9562151627259001 |
| Encrypted: | false |
| SSDEEP: | 24576:1dLv1SxfFUaWse9zZi2Ou/iDyUOjoEO3PX2BU:2UagzU2Ouj |
| MD5: | 35192049828138889E770C6215309EF4 |
| SHA1: | 3DEF216321EAF2E148E9C43916AF7E46C31A494C |
| SHA-256: | BC723EA305392B9CA08507036BF2A0DDBDFF2455E2B37793BCD7635BF26C6290 |
| SHA-512: | 1532788E22E67A73FC436ABF7315FC04FA12C63EA0E9A8D59F881476B95383F2D479A13694F24D6AA3B514E9F2391E2EE5E72B9267D53A803E32C2E617D4D40D |
| Malicious: | false |
| Reputation: | low |
| Preview: | \|..... .....v1.....l~..".."...wK.....m.....%....y=.&....y..h.o.....k.\."...w.....Y.....B..... ..... .....&....y{..... .....W.+....y.....~...*....y..... ..... |

| C:\Users\user\AppData\Local\Temp\tmpBCAF.tmp | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe |
| File Type: | Little-endian UTF-16 Unicode text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 2 |
| Entropy (8bit): | 1.0 |
| Encrypted: | false |
| SSDEEP: | 3:Qn:Qn |
| MD5: | F3B25701FE362EC84616A93A45CE9998 |
| SHA1: | D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB |
| SHA-256: | B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209 |
| SHA-512: | 98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4 |
| Malicious: | false |
| Reputation: | high, very likely benign file |

| C:\Users\user\AppData\Local\Temp\tmpBCAF.tmp | |
|---|---|
| Preview: | .. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 6.134409482814605 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | SecuriteInfo.com.Trojan.AutoIt.316.10986.exe |
| File size: | 2135040 |
| MD5: | 52d4245d65d5cc2da05298c480ffcc5f |
| SHA1: | b2ecf335eb93feba2cf923419e70d7b6cff79061 |
| SHA256: | 70ef3c88a90dd590de9a0ac4634b5017f35ea6dedec14f3cc3b5d9eeb3ca84a2 |
| SHA512: | ab847b2e12b9ef8e494688094260967f42f8c0dc6797d635162b64fb32ac8720a2051441128b5a0528eeabe0fc8f5b8dafda15d688721037a2734e5e0629b02f |
| SSDEEP: | 24576:8AHnh+eWsN3skA4RV1Hom2KXMmHaurntQLuyoI4f+O2fRHonhhlvXGE3nR5:bh+ZkldoPK8Yaux3b |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..R...R...R....C..P.....;.S..._@#.a..._@....._@..g...[j..[...[jo.w...R...r.....#.S..._@'.S...R.k.S.....".S...RichR.. |

## File Icon

| | |
|---|---|
| Icon Hash: | c4c4ccccccd4d2ec |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x42800a |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE |
| DLL Characteristics: | TERMINAL_SERVER_AWARE, DYNAMIC_BASE |
| Time Stamp: | 0x5C503AC3 [Tue Jan 29 11:36:35 2019 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 1 |
| File Version Major: | 5 |
| File Version Minor: | 1 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 1 |
| Import Hash: | afcdf79be1557326c854b6e20cb900a7 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x8dfdd | 0x8e000 | False | 0.573560258033 | data | 6.67524835171 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x8f000 | 0x2fd8e | 0x2fe00 | False | 0.328288185379 | data | 5.76324400576 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xbf000 | 0x8f74 | 0x5200 | False | 0.10175304878 | data | 1.19638192355 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xc8000 | 0x13ecb4 | 0x13ee00 | False | 0.579503136025 | data | 4.90682884361 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x207000 | 0x7134 | 0x7200 | False | 0.761753015351 | data | 6.78395555713 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

### Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | Great Britain |  |

### Static AutoIT Info

## Network Behavior

**No network behavior found**

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: SecuriteInfo.com.Trojan.AutoIt.316.10986.exe PID: 4720 Parent PID: 6040

### General

| | |
|---|---|
| Start time: | 14:15:51 |
| Start date: | 10/12/2021 |
| Path: | C:\Users\user\Desktop\SecuriteInfo.com.Trojan.AutoIt.316.10986.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.AutoIt.316.10986.exe" |
| Imagebase: | 0xd00000 |
| File size: | 2135040 bytes |
| MD5 hash: | 52D4245D65D5CC2DA05298C480FFCC5F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000003.248337037.0000000000FF0000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000003.248337037.0000000000FF0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000003.251645855.0000000000FF2000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000003.251645855.0000000000FF2000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

## Analysis Process: RegAsm.exe PID: 5908 Parent PID: 4720

### General

| | |
|---|---|
| Start time: | 14:15:53 |
| Start date: | 10/12/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe |
| Imagebase: | 0xb80000 |
| File size: | 53248 bytes |
| MD5 hash: | 529695608EAFBED00ACA9E61EF333A7C |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

| | |
|---|---|
| Yara matches: | • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000000.252098069.0000000000402000.00000020.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000000.252098069.0000000000402000.00000020.00000001.sdmp, Author: Joe Security<br>• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.516270179.00000000031E9000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.516270179.00000000031E9000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.519365892.0000000006D51000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.519365892.0000000006D51000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000000.251237840.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000000.251237840.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.516610948.0000000003292000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.514267996.0000000000402000.00000020.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.514267996.0000000000402000.00000020.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000003.253770360.0000000004A43000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000003.253770360.0000000004A43000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000001.00000002.518879964.00000000051D0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.518879964.00000000051D0000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.518879964.00000000051D0000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.518219732.00000000033CE000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | high |

## File Activities

Show Windows behavior

### File Created

### File Deleted

### File Written

### File Read

## Analysis Process: vbc.exe PID: 4484 Parent PID: 5908

### General

| | |
|---|---|
| Start time: | 14:15:56 |
| Start date: | 10/12/2021 |

| | |
|---|---|
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\App Data\Local\Temp\tmpBCAF.tmp |
| Imagebase: | 0x400000 |
| File size: | 1171592 bytes |
| MD5 hash: | C63ED21D5706A527419C9FBD730FFB2E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000000.261547769.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000000.262035406.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000000.261098528.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000000.260466252.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.273168143.0000000000400000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: vbc.exe PID: 5964 Parent PID: 5908

### General

| | |
|---|---|
| Start time: | 14:17:02 |
| Start date: | 10/12/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\App Data\Local\Temp\tmpBBC1.tmp |
| Imagebase: | 0x400000 |
| File size: | 1171592 bytes |
| MD5 hash: | C63ED21D5706A527419C9FBD730FFB2E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000000.401565016.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.401565016.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000000.401266886.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.401266886.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000002.403068621.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000002.403068621.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000000.401896100.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.401896100.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000000.402276978.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.402276978.0000000000400000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | high |

# Disassembly

## Code Analysis