

JOeSandbox Cloud BASIC



**ID:** 356587

**Sample Name:**

SecuriteInfo.com.Trojan.GenericKDZ.73120.139.15119

**Cookbook:** default.jbs

**Time:** 11:49:30

**Date:** 23/02/2021

**Version:** 31.0.0 Emerald

# Table of Contents

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Table of Contents                                                  | 2  |
| Analysis Report SecuriteInfo.com.Trojan.GenericKDZ.73120.139.15119 | 4  |
| Overview                                                           | 4  |
| General Information                                                | 4  |
| Detection                                                          | 4  |
| Signatures                                                         | 4  |
| Classification                                                     | 4  |
| Startup                                                            | 4  |
| Malware Configuration                                              | 4  |
| Threatname: FormBook                                               | 4  |
| Yara Overview                                                      | 5  |
| Memory Dumps                                                       | 5  |
| Unpacked PEs                                                       | 6  |
| Sigma Overview                                                     | 7  |
| Signature Overview                                                 | 7  |
| AV Detection:                                                      | 7  |
| Compliance:                                                        | 7  |
| Networking:                                                        | 7  |
| E-Banking Fraud:                                                   | 7  |
| System Summary:                                                    | 8  |
| Data Obfuscation:                                                  | 8  |
| Malware Analysis System Evasion:                                   | 8  |
| Stealing of Sensitive Information:                                 | 8  |
| Remote Access Functionality:                                       | 8  |
| Mitre Att&ck Matrix                                                | 8  |
| Behavior Graph                                                     | 8  |
| Screenshots                                                        | 9  |
| Thumbnails                                                         | 9  |
| Antivirus, Machine Learning and Genetic Malware Detection          | 10 |
| Initial Sample                                                     | 10 |
| Dropped Files                                                      | 10 |
| Unpacked PE Files                                                  | 10 |
| Domains                                                            | 10 |
| URLs                                                               | 10 |
| Domains and IPs                                                    | 11 |
| Contacted Domains                                                  | 11 |
| Contacted URLs                                                     | 11 |
| URLs from Memory and Binaries                                      | 11 |
| Contacted IPs                                                      | 11 |
| General Information                                                | 11 |
| Simulations                                                        | 12 |
| Behavior and APIs                                                  | 12 |
| Joe Sandbox View / Context                                         | 12 |
| IPs                                                                | 12 |
| Domains                                                            | 12 |
| ASN                                                                | 12 |
| JA3 Fingerprints                                                   | 12 |
| Dropped Files                                                      | 12 |
| Created / dropped Files                                            | 12 |
| Static File Info                                                   | 13 |
| General                                                            | 13 |
| File Icon                                                          | 13 |
| Static PE Info                                                     | 13 |
| General                                                            | 13 |
| Entrypoint Preview                                                 | 14 |
| Data Directories                                                   | 15 |

|                                                                                               |           |
|-----------------------------------------------------------------------------------------------|-----------|
| Sections                                                                                      | 15        |
| Resources                                                                                     | 16        |
| Imports                                                                                       | 16        |
| Version Infos                                                                                 | 16        |
| <b>Network Behavior</b>                                                                       | <b>16</b> |
| <b>Code Manipulations</b>                                                                     | <b>16</b> |
| <b>Statistics</b>                                                                             | <b>16</b> |
| Behavior                                                                                      | 16        |
| <b>System Behavior</b>                                                                        | <b>17</b> |
| Analysis Process: SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe PID: 6528 Parent PID: 5608 | 17        |
| General                                                                                       | 17        |
| File Activities                                                                               | 17        |
| File Created                                                                                  | 17        |
| File Written                                                                                  | 18        |
| File Read                                                                                     | 18        |
| Analysis Process: SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe PID: 6652 Parent PID: 6528 | 19        |
| General                                                                                       | 19        |
| File Activities                                                                               | 19        |
| File Read                                                                                     | 19        |
| <b>Disassembly</b>                                                                            | <b>19</b> |
| Code Analysis                                                                                 | 19        |

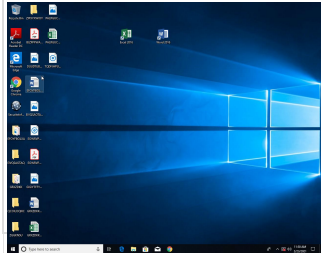
# Analysis Report SecuriteInfo.com.Trojan.GenericKDZ.73...

## Overview

General Information

|              |                                                                                                |
|--------------|------------------------------------------------------------------------------------------------|
| Sample Name: | SecuriteInfo.com.Trojan.GenericKDZ.73120.139.15119 (renamed file extension from 151119 to exe) |
| Analysis ID: | 356587                                                                                         |
| MD5:         | fac509b5175d364.                                                                               |
| SHA1:        | 048a87d3a93821..                                                                               |
| SHA256:      | 44283ee3be33ad..                                                                               |

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

FormBook

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

Signatures

Found malware configuration

Malicious sample detected (through ...

Multi AV Scanner detection for subm...

Yara detected AntiVM\_3

Yara detected FormBook

.NET source code contains potentia...

.NET source code contains very larg...

C2 URLs / IPs found in malware con...

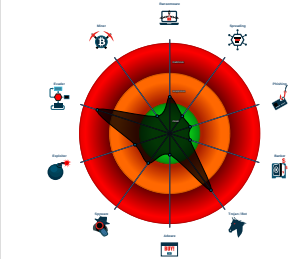
Machine Learning detection for samp...

Tries to detect sandboxes and other...

Tries to detect virtualization through...

Antivirus or Machine Learning detec...

Classification



## Startup

- System is w10x64
-  [SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe](#) (PID: 6528 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe' MD5: FAC509B5175D3647945BDBF7AC010ACC)
  -  [SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe](#) (PID: 6652 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe MD5: FAC509B5175D3647945BDBF7AC010ACC)
- cleanup

## Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rizrvd.com/bw82/"
  ],
  "decoy": [
    "fundamentalienef.com",
    "gallerybrows.com",
    "leadeligey.com",
    "octoberx2.online",
    "climaxnovels.com",
    "gdsjgf.com",
    "curateherstories.com",
    "blacksailus.com",
    "yjpps.com",
    "gmobilet.com",
    "fcoins.club",
    "foreverlive2027.com",
    "healthyfifties.com",
    "wmarquezy.com",
    "housebulb.com",
    "thebabyfriendly.com",
    "primajayaintiperkasa.com",
    "learnplaychess.com",
    "chrisbubser.digital",
    "xn--avenr-wsa.com",
    "exlineinsurance.com",
    "thrivezi.com",
    "tuvandadayvitos24h.online",
    "illfingers.com",
    "usmedicarenow.com",
    "pandabutik.com",
    "engageautism.info",
    "magnabeautystyle.com",
    "texasdryroof.com",
    "woodlandpizzahartford.com",
    "dameadamea.com",
    "sedaskincare.com",
    "ruysatu99.com",
    "mybestaide.com",
    "nikolaichan.com",
    "mrcabinetkitchenandbath.com",
    "ondemandbarbering.com",
    "activagebenefits.net",
    "srcsvcs.com",
    "cbrealitalize.com",
    "ismaelworks.com",
    "medkomp.online",
    "ninasangtani.com",
    "h2oturkiye.com",
    "kolamart.com",
    "acdfr.com",
    "twistedtailgatesweeps1.com",
    "ramjamdee.com",
    "thedancehalo.com",
    "joeisono.com",
    "glasshouseroadtrip.com",
    "okcpp.com",
    "riggsfarmfenceservices.com",
    "mgg360.com",
    "xn--oi2b190cymc.com",
    "ctfocbdwholesale.com",
    "openspiers.com",
    "rumblingrambles.com",
    "thepoetrictedstudio.com",
    "magiclabs.media",
    "wellnesssensation.com",
    "lakegastonautoparts.com",
    "dealsonwheeles.com",
    "semenboostplus.com"
  ]
}
```

## Yara Overview

### Memory Dumps

| Source                                                              | Rule                 | Description            | Author       | Strings |
|---------------------------------------------------------------------|----------------------|------------------------|--------------|---------|
| 00000002.00000002.224039712.0000000000400000.0000040.000000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security |         |

| Source                                                               | Rule                 | Description                                        | Author                                               | Strings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------|----------------------|----------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 00000002.00000002.224039712.0000000000400000.0000040.00000001.sdmp   | Formbook_1           | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | <ul style="list-style-type: none"> <li>• 0x85e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x8972:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x14685:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li> <li>• 0x14171:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>• 0x14787:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>• 0x148ff:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>• 0x938a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>• 0x133ec:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>• 0xa102:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>• 0x19777:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>• 0x1a81a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 00000002.00000002.224039712.0000000000400000.0000040.00000001.sdmp   | Formbook             | detect Formbook in memory                          | JPCERT/CC Incident Response Group                    | <ul style="list-style-type: none"> <li>• 0x166a9:\$sqlite3step: 68 34 1C 7B E1</li> <li>• 0x167bc:\$sqlite3step: 68 34 1C 7B E1</li> <li>• 0x166d8:\$sqlite3text: 68 38 2A 90 C5</li> <li>• 0x167fd:\$sqlite3text: 68 38 2A 90 C5</li> <li>• 0x166eb:\$sqlite3blob: 68 53 D8 7F 8C</li> <li>• 0x16813:\$sqlite3blob: 68 53 D8 7F 8C</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 00000000.00000002.224800988.000000000036E9000.00000004.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook                             | Joe Security                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 00000000.00000002.224800988.000000000036E9000.00000004.00000001.sdmp | Formbook_1           | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | <ul style="list-style-type: none"> <li>• 0x254eb8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x255242:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x27c0d8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x27c462:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x260f55:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94</li> <li>• 0x288175:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94</li> <li>• 0x260a41:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>• 0x287c61:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>• 0x261057:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>• 0x288277:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>• 0x2611cf:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>• 0x2883ef:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>• 0x255c5a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>• 0x27ce7a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>• 0x25fcbc:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>• 0x286edc:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F 8</li> <li>• 0x2569d2:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>• 0x27dbf2:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>• 0x266047:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>• 0x28d267:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>• 0x2670ea:\$sequence_9: 56 68 03 01 00 00 8D 85 95 F E FF FF 6A 00</li> </ul> |
| Click to see the 3 entries                                           |                      |                                                    |                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Unpacked PEs

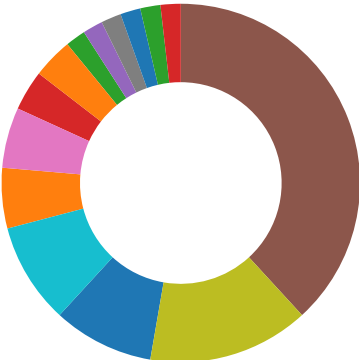
| Source                                                                   | Rule                 | Description                                        | Author                                               | Strings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------|----------------------|----------------------------------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.400000.0.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook                             | Joe Security                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.400000.0.raw.unpack | Formbook_1           | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | <ul style="list-style-type: none"> <li>• 0x85e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x8972:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>• 0x14685:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li> <li>• 0x14171:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>• 0x14787:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>• 0x148ff:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>• 0x938a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>• 0x133ec:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>• 0xa102:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>• 0x19777:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>• 0x1a81a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00</li> </ul> |
| 2.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.400000.0.raw.unpack | Formbook             | detect Formbook in memory                          | JPCERT/CC Incident Response Group                    | <ul style="list-style-type: none"> <li>• 0x166a9:\$sqlite3step: 68 34 1C 7B E1</li> <li>• 0x167bc:\$sqlite3step: 68 34 1C 7B E1</li> <li>• 0x166d8:\$sqlite3text: 68 38 2A 90 C5</li> <li>• 0x167fd:\$sqlite3text: 68 38 2A 90 C5</li> <li>• 0x166eb:\$sqlite3blob: 68 53 D8 7F 8C</li> <li>• 0x16813:\$sqlite3blob: 68 53 D8 7F 8C</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.400000.0.unpack     | JoeSecurity_FormBook | Yara detected FormBook                             | Joe Security                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Source                                                               | Rule       | Description                                        | Author                                               | Strings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------|------------|----------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.400000.0.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | <ul style="list-style-type: none"> <li>0x77e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x7b72:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x13885:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li> <li>0x13371:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>0x13987:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>0x13aff:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>0x858a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>0x125ec:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>0x9302:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>0x18977:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>0x19a1a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00</li> </ul> |
| Click to see the 8 entries                                           |            |                                                    |                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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 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:



System Summary:



Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:



.NET source code contains potential unpacker

Malware Analysis System Evasion:



Yara detected AntiVM\_3

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

Tries to detect virtualization through RDTSC time measurements

Stealing of Sensitive Information:



Yara detected FormBook

Remote Access Functionality:

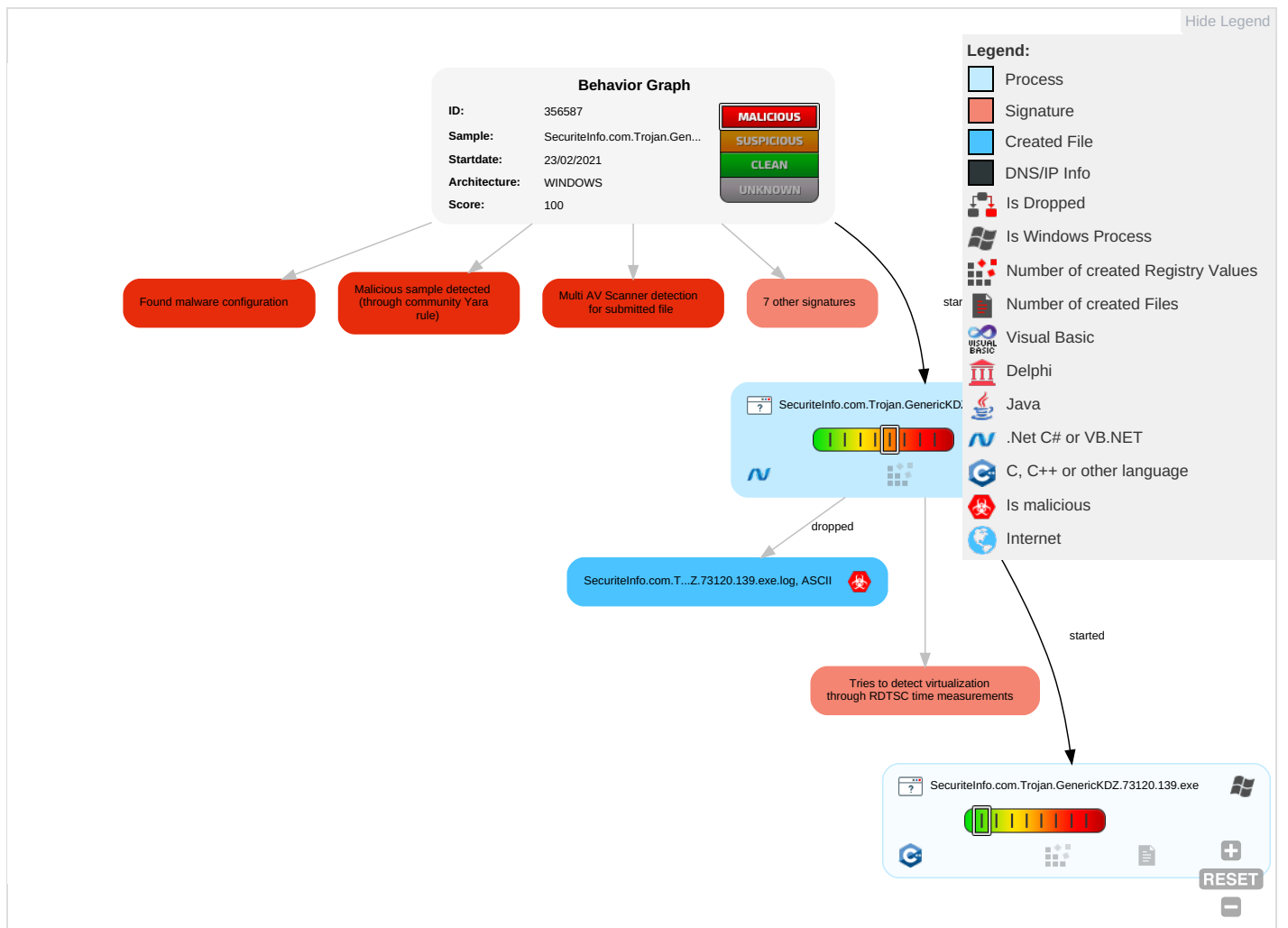


Yara detected FormBook

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                      | Windows Management Instrumentation | Path Interception                    | Process Injection 1 1                | Masquerading 1                            | OS Credential Dumping     | Security Software Discovery 2 2 1  | Remote Services                    | Archive Collected Data 1       | Exfiltration Over Other Network Medium | Encrypted Channel 1          | Eavesdrop on Insecure Network Communication |
| Default Accounts                    | Scheduled Task/Job                 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 3          | LSASS Memory              | Virtualization/Sandbox Evasion 3   | Remote Desktop Protocol            | Data from Removable Media      | Exfiltration Over Bluetooth            | Application Layer Protocol 1 | Exploit SS7 to Redirect Phone Calls/SMS     |
| Domain Accounts                     | At (Linux)                         | Logon Script (Windows)               | Logon Script (Windows)               | Disable or Modify Tools 1                 | Security Account Manager  | Process Discovery 1                | 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)                   | Process Injection 1 1                     | NTDS                      | System Information Discovery 1 1 2 | Distributed Component Object Model | Input Capture                  | Scheduled Transfer                     | Protocol Impersonation       | SIM Card Swap                               |
| Cloud Accounts                      | Cron                               | Network Logon Script                 | Network Logon Script                 | Deobfuscate/Decode Files or Information 1 | LSA Secrets               | Remote System Discovery            | SSH                                | Keylogging                     | Data Transfer Size Limits              | Fallback Channels            | Manipulate Device Communication             |
| Replication Through Removable Media | Launchd                            | Rc.common                            | Rc.common                            | Obfuscated Files or Information 4 1       | Cached Domain Credentials | System Owner/User Discovery        | VNC                                | GUI Input Capture              | Exfiltration Over C2 Channel           | Multiband Communication      | Jamming or Denial of Service                |
| External Remote Services            | Scheduled Task                     | Startup Items                        | Startup Items                        | Software Packing 1 2                      | DCSync                    | Network Sniffing                   | Windows Remote Management          | Web Portal Capture             | Exfiltration Over Alternative Protocol | Commonly Used Port           | Rogue Wi-Fi Access Point                    |

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.GenericKDZ.73120.139.exe | 37%       | Virustotal     |                         | <a href="#">Browse</a> |
| SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe | 30%       | ReversingLabs  | Win32.Trojan.AgentTesla |                        |
| SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe | 100%      | Joe Sandbox ML |                         |                        |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source                                                               | Detection | Scanner | Label              | Link | Download                      |
|----------------------------------------------------------------------|-----------|---------|--------------------|------|-------------------------------|
| 2.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.400000.0.unpack | 100%      | Avira   | TR/Crypt.ZPACK.Gen |      | <a href="#">Download File</a> |

### Domains

No Antivirus matches

### URLs

| Source               | Detection | Scanner         | Label | Link |
|----------------------|-----------|-----------------|-------|------|
| www.rizrvd.com/bw82/ | 0%        | Avira URL Cloud | safe  |      |

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

| Name                 | Malicious | Antivirus Detection                                                   | Reputation |
|----------------------|-----------|-----------------------------------------------------------------------|------------|
| www.rizrvd.com/bw82/ | true      | <ul style="list-style-type: none"><li>Avira URL Cloud: safe</li></ul> | low        |

### URLs from Memory and Binaries

| Name                                                                                    | Source                                                                                                                            | Malicious | Antivirus Detection | Reputation |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------|---------------------|------------|
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name                              | SecuriteInfo.com.Trojan.Generi<br>cKDZ.73120.139.exe, 00000000.0<br>0000002.224526375.00000000026E<br>1000.00000004.00000001.sdmp | false     |                     | high       |
| http://<br>https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstr<br>ap.min.css | SecuriteInfo.com.Trojan.Generi<br>cKDZ.73120.139.exe, 00000000.0<br>0000002.224526375.00000000026E<br>1000.00000004.00000001.sdmp | false     |                     | high       |

### Contacted IPs

No contacted IP infos

## General Information

|                                                    |                                                                                                                                                                            |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 31.0.0 Emerald                                                                                                                                                             |
| Analysis ID:                                       | 356587                                                                                                                                                                     |
| Start date:                                        | 23.02.2021                                                                                                                                                                 |
| Start time:                                        | 11:49:30                                                                                                                                                                   |
| Joe Sandbox Product:                               | CloudBasic                                                                                                                                                                 |
| Overall analysis duration:                         | 0h 6m 10s                                                                                                                                                                  |
| Hypervisor based Inspection enabled:               | false                                                                                                                                                                      |
| Report type:                                       | light                                                                                                                                                                      |
| Sample file name:                                  | SecuriteInfo.com.Trojan.GenericKDZ.73120.139.15119<br>(renamed file extension from 15119 to exe)                                                                           |
| Cookbook file name:                                | default.jbs                                                                                                                                                                |
| Analysis system description:                       | Windows 10 64 bit v1803 with Office Professional Plus<br>2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8<br>Update 211                                                  |
| Number of analysed new started processes analysed: | 4                                                                                                                                                                          |
| 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:                                      | <ul style="list-style-type: none"><li>HCA enabled</li><li>EGA enabled</li><li>HDC enabled</li><li>AMSI enabled</li></ul>                                                   |
| Analysis Mode:                                     | default                                                                                                                                                                    |
| Analysis stop reason:                              | Timeout                                                                                                                                                                    |
| Detection:                                         | MAL                                                                                                                                                                        |
| Classification:                                    | mal100.troj.evad.winEXE@3/1@0/0                                                                                                                                            |
| EGA Information:                                   | Failed                                                                                                                                                                     |
| HDC Information:                                   | <ul style="list-style-type: none"><li>Successful, ratio: 2.9% (good quality ratio 2.9%)</li><li>Quality average: 72.5%</li><li>Quality standard deviation: 28.3%</li></ul> |

|                    |                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HCA Information:   | <ul style="list-style-type: none"><li>• Successful, ratio: 99%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul> |
| Cookbook Comments: | <ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Stop behavior analysis, all processes terminated</li></ul>              |
| Warnings:          | Show All <ul style="list-style-type: none"><li>• Exclude process from analysis (whitelisted): taskhostw.exe, svchost.exe</li></ul>                               |

## Simulations

### Behavior and APIs

| Time     | Type            | Description                                                                          |
|----------|-----------------|--------------------------------------------------------------------------------------|
| 11:50:25 | API Interceptor | 1x Sleep call for process: SecuriteInfo.com.Trojan.GenericKDZ.73120.139.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\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.log |                                                                                                                                 |
| Process:                                                                                                         | C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe                                                          |
| File Type:                                                                                                       | ASCII text, with CRLF line terminators                                                                                          |
| Category:                                                                                                        | dropped                                                                                                                         |
| Size (bytes):                                                                                                    | 1314                                                                                                                            |
| Entropy (8bit):                                                                                                  | 5.350128552078965                                                                                                               |
| Encrypted:                                                                                                       | false                                                                                                                           |
| SSDEEP:                                                                                                          | 24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR                            |
| MD5:                                                                                                             | 1DC1A2DCC9EFAA84EABF4F6D6066565B                                                                                                |
| SHA1:                                                                                                            | B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9                                                                                        |
| SHA-256:                                                                                                         | 28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEf                                                                |
| SHA-512:                                                                                                         | 95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7 |
| Malicious:                                                                                                       | true                                                                                                                            |
| Reputation:                                                                                                      | high, very likely benign file                                                                                                   |



|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\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\fd1d8480152e0da9a60ad49c6d16a3b6d\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=b77a |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Static File Info

### General

|                       |                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File type:            | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows                                                                                                                                                                                                                                                                     |
| Entropy (8bit):       | 6.784399876642811                                                                                                                                                                                                                                                                                                                        |
| TrID:                 | <ul style="list-style-type: none"><li>Win32 Executable (generic) Net Framework (10011505/4) 49.80%</li><li>Win32 Executable (generic) a (10002005/4) 49.75%</li><li>Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%</li><li>Windows Screen Saver (13104/52) 0.07%</li><li>Generic Win/DOS Executable (2004/3) 0.01%</li></ul> |
| File name:            | SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe                                                                                                                                                                                                                                                                                         |
| File size:            | 1044992                                                                                                                                                                                                                                                                                                                                  |
| MD5:                  | fac509b5175d3647945bdf7ac010acc                                                                                                                                                                                                                                                                                                          |
| SHA1:                 | 048a87d3a938217f555da58662da7bfe59971a9e                                                                                                                                                                                                                                                                                                 |
| SHA256:               | 44283ee3be33ad2077f6c8c18b1699f3d694cb936336523b299646f1a39ea8fc                                                                                                                                                                                                                                                                         |
| SHA512:               | e6965ff1f36abdbc2c8903c6263e941daf9cea7c7b27a9c7e4cca4d31bc931a3df6b0951014d5ab40985d31c698d1588a1943cf6862c290dc0e18198a7b29657                                                                                                                                                                                                         |
| SSDEEP:               | 12288:U1adigOaHhw5Lk+hg2iwndbVSdmPFkvvu3LmAkt3fkGL6Dv6u/ZHmSYrRBmR2v:UbaAx3domFKuy5Ts+CuB6rRMR2                                                                                                                                                                                                                                          |
| File Content Preview: | MZ.....@.....!..L.!Th<br>is program cannot be run in DOS mode....\$......PE..L.....<br>3'.....P.....L.....@.....`.....<br>..@.....                                                                                                                                                                                                       |

### File Icon

|            |                  |
|------------|------------------|
|            |                  |
| Icon Hash: | 71e8e4a8e8f634c0 |

### Static PE Info

#### General

|                             |                                                        |
|-----------------------------|--------------------------------------------------------|
| Entrypoint:                 | 0x4fc2c2                                               |
| Entrypoint Section:         | .text                                                  |
| Digitally signed:           | false                                                  |
| Imagebase:                  | 0x400000                                               |
| Subsystem:                  | windows gui                                            |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE                        |
| DLL Characteristics:        | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp:                 | 0x603383DB [Mon Feb 22 10:13:47 2021 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                       |

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

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



| Name   | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy        | Characteristics                                                               |
|--------|-----------------|--------------|----------|----------|-----------------|-----------|----------------|-------------------------------------------------------------------------------|
| .reloc | 0x104000        | 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       | 0xfe100  | 0x4228 | dBase III DBT, version number 0, next free block index 40                   |          |         |
| RT_GROUP_ICON | 0x102338 | 0x14   | data                                                                        |          |         |
| RT_VERSION    | 0x10235c | 0x3a6  | data                                                                        |          |         |
| RT_MANIFEST   | 0x102714 | 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   | Copyright 2017 Robert B. Cialdini |
| Assembly Version | 43.338.0.0                        |
| InternalName     | CLRSurrogateEntry.exe             |
| FileVersion      | 43.338.0.0                        |
| CompanyName      | Robert B. Cialdini                |
| LegalTrademarks  |                                   |
| Comments         |                                   |
| ProductName      | Thesis Nana                       |
| ProductVersion   | 43.338.0.0                        |
| FileDescription  | Thesis Nana                       |
| OriginalFilename | CLRSurrogateEntry.exe             |

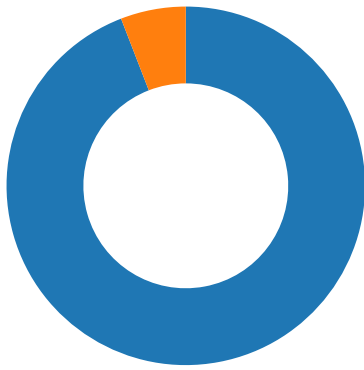
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

## System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe PID: 6528  
Parent PID: 5608

### General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 11:50:24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Start date:                   | 23/02/2021                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Path:                         | C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Wow64 process (32bit):        | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Commandline:                  | 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe'                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Imagebase:                    | 0x230000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File size:                    | 1044992 bytes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MD5 hash:                     | FAC509B5175D3647945BDBF7AC010ACC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Programmed in:                | .Net C# or VB.NET                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.224800988.00000000036E9000.00000004.00000001.sdmp, Author: Joe Security</li><li>Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.224800988.00000000036E9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.224800988.00000000036E9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li><li>Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.224526375.00000000026E1000.00000004.00000001.sdmp, Author: Joe Security</li></ul> |
| 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     | 6E0FCF06       | unknown |

| File Path                                                                                                        | Access                                        | Attributes | Options                                                                                | Completion            | Count | Source Address | Symbol      |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|------------|----------------------------------------------------------------------------------------|-----------------------|-------|----------------|-------------|
| 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     | 6E0FCF06       | unknown     |
| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.log | read attributes   synchronize   generic write | device     | synchronous io non alert   non directory file                                          | success or wait       | 1     | 6E40C78D       | CreateFileW |

#### File Written

| File Path                                                                                                        | Offset  | Length | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Ascii                                                                                                                                                                                                                                                                                 | Completion      | Count | Source Address | Symbol    |
|------------------------------------------------------------------------------------------------------------------|---------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------|----------------|-----------|
| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe.log | unknown | 1314   | 31 2c 22 66 75 73 69<br>6f 6e 22 2c 22 47 41<br>43 22 2c 30 0d 0a 31<br>2c 22 57 69 6e 52 54<br>22 2c 22 4e 6f 74 41<br>70 70 22 2c 31 0d 0a<br>32 2c 22 4d 69 63 72<br>6f 73 6f 66 74 2e 56<br>69 73 75 61 6c 42 61<br>73 69 63 2c 20 56 65<br>72 73 69 6f 6e 3d 31<br>30 2e 30 2e 30 2e 30<br>2c 20 43 75 6c 74 75<br>72 65 3d 6e 65 75 74<br>72 61 6c 2c 20 50 75<br>62 6c 69 63 4b 65 79<br>54 6f 6b 65 6e 3d 62<br>30 33 66 35 66 37 66<br>31 31 64 35 30 61 33<br>61 22 2c 30 0d 0a 32<br>2c 22 53 79 73 74 65<br>6d 2e 57 69 6e 64 6f<br>77 73 2e 46 6f 72 6d<br>73 2c 20 56 65 72 73<br>69 6f 6e 3d 34 2e 30<br>2e 30 2e 30 2c 20 43<br>75 6c 74 75 72 65 3d<br>6e 65 75 74 72 61 6c<br>2c 20 50 75 62 6c 69<br>63 4b 65 79 54 6f 6b<br>65 6e 3d 62 37 37 61<br>35 63 35 36 31 39 33<br>34 65 30 38 39 22 2c<br>30 0d 0a 33 2c 22 53<br>79 73 74 65 6d 2c 20<br>56 65 72 73 69 6f 6e<br>3d 34 2e | 1,"fusion","GAC",0..1,"WinRT",<br>"NotApp",1..2,"Microsoft.VisualStudioBasic,<br>Version=10.0.0.0, Culture=neutral,<br>PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms,<br>Version=4.0.0.0, Culture=neutral,<br>PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4. | success or wait | 1     | 6E40C907       | 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     | 6E0D5705       | unknown  |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config                                                                  | unknown | 6135   | success or wait | 1     | 6E0D5705       | unknown  |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux                         | unknown | 176    | success or wait | 1     | 6E0303DE       | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config                                                                  | unknown | 4095   | success or wait | 1     | 6E0DCA54       | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux                             | unknown | 620    | success or wait | 1     | 6E0303DE       | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux | unknown | 864    | success or wait | 1     | 6E0303DE       | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux                    | unknown | 900    | success or wait | 1     | 6E0303DE       | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux                     | unknown | 748    | success or wait | 1     | 6E0303DE       | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config                                                                  | unknown | 4095   | success or wait | 1     | 6E0D5705       | unknown  |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config                                                                  | unknown | 8171   | end of file     | 1     | 6E0D5705       | unknown  |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config                                                                  | unknown | 4096   | success or wait | 1     | 6CF41B4F       | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config                                                                  | unknown | 4096   | end of file     | 1     | 6CF41B4F       | ReadFile |

## General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 11:50:26                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Start date:                   | 23/02/2021                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Path:                         | C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Wow64 process (32bit):        | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Commandline:                  | C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.139.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Imagebase:                    | 0x770000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| File size:                    | 1044992 bytes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MD5 hash:                     | FAC509B5175D3647945BDBF7AC010ACC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.224039712.0000000000400000.00000040.00000001.sdmp, Author: Joe Security</li><li>Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.224039712.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.224039712.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li></ul> |
| 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     | 4182A7         | NtReadFile |

## Disassembly

## Code Analysis