

# Digital artists targeted in RedLine infostealer campaign

---

 [bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.html](https://bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.html)

*2021-06-17: updated with information from Twitter user ARC*

In this post, we'll look at a campaign, that targeted multiple 3D or digital artists using NFT, with malware named **RedLine**. This malware is a so called "infostealer" or "information stealer" that is capable of extracting sensitive data from your machine (such as wallet information, credentials, and so on). As a side-note; NFTs, or non-fungible tokens, are digital tokens tied to assets that can be bought, sold and traded.

This blog post is divided into four parts:

- Introduction: provides an overview of what happened
- Analysis: analysis of the attack and the malware used
- Detection: how to detect and remove the malware (skip to Detection if you just want to clean this up)
- Prevention: how to prevent this from happening again
- Conclusion: a brief conclusion and additional thoughts



## Introduction

---

From at least last Thursday, 10th of June 2021, multiple users report on Twitter that they got hacked after being approached to create new digital art. These users, accomplished digital artists and publishing their work on NFT marketplaces, were approached either via Instagram, Twitter DM (message) or directly via email. The attacker has masqueraded themselves behind multiple personas, often claiming to be from South Korea. A few of the users that reported the attack:

Ariel:

Small thread on the recent attacks to NFT artists, and how to prevent it. [#NFTLamers](#) [#StolenNFT](#) [#NFTArt](#) [pic.twitter.com/KvrsuyQaeT](https://pic.twitter.com/KvrsuyQaeT)

—  ArielBeckerArt.eth #SquidGang  (@arielbeckerart) [June 10, 2021](#)

fvckrender:

Be really careful out there I was dumb enough to not overlook this and open their SCR file and got my metamask swiped from à to Z all my tokens gone. They tried to access other app but my 2fa blocked them to. I'm an idiot don't me an idiot like me and secure your shit. [pic.twitter.com/gAins00taH](https://pic.twitter.com/gAins00taH)

— FVCKRENDER (@fvckrender) [June 11, 2021](#)

Nicole:

Really terrible day. My Metamask got hacked and now my [@withFND](#) account is compromised. Opened a scam project proposal with a .scr file and a Microsoft Word icon. Anyone experience this before? Trying to figure out what to do

— Nicole Ruggiero (@\_NicoleRuggiero) [June 11, 2021](#)

ARC:

New scam just dropped, specifically targeting artists, the file seems to be a virus [pic.twitter.com/IFv8N5RBSg](https://pic.twitter.com/IFv8N5RBSg)

— ARC (@arc4g) [June 11, 2021](#)

Cloudy Night:

WARNING TO ALL ARTISTS

Got a DM from "John Billmate" claiming to be "Responsible for distribution of photo editor" from [@SkylumSoftware](#)

DO NOT OPEN ANY LINKS FROM THIS PERSON. This is a scam, and if you got this DM, or get a dm in the future, block it. [#NFTCommunity](#) [#skylum](#)  
[pic.twitter.com/yQv68bRljW](https://pic.twitter.com/yQv68bRljW)

— Cloudy Night 🌩️ (@CloudyNight\_k) [June 11, 2021](#)

There are many, many more examples - however, we won't list them here. Of note is Ariel's tweet, where you can note the presence of a file named "**Rizin\_Fight\_Federation\_Presentation.scr**". I'll circle back to that in the next section, Analysis.

## Analysis

After scouring the internet for a while, I was unable to discover any of the files mentioned by the artists that reported the attack, that is until I stumbled upon Cloudy Night's tweet - their screenshot included a link to a website "skylumpro.com".



As expected, this is not the legitimate website, but rather a clever copycat of the real Skylum product website (to note, the real website is: <https://skylum.com/luminar-ai-b>). After clicking the "Download Now" button, a file named "**SkylumLuminar (NFT Beta).rar**" is downloaded, which you need to unzip with the password "NFT", as we can observe from Cloudy Night's tweet.

The unzipped content looks as follows:

Name	Date modified	Type	Size
de-DE	13/06/2021 00:40	File folder	
en-US	13/06/2021 00:40	File folder	
es-ES	13/06/2021 00:40	File folder	
fr-FR	13/06/2021 00:40	File folder	
hi-HI	13/06/2021 00:40	File folder	
hu-HU	13/06/2021 00:40	File folder	
in-IN	13/06/2021 00:40	File folder	
it-IT	13/06/2021 00:40	File folder	
ja-JP	13/06/2021 00:40	File folder	
ko-KR	13/06/2021 00:40	File folder	
platforms	13/06/2021 00:40	File folder	
pl-PL	13/06/2021 00:40	File folder	
pt-BR	13/06/2021 00:40	File folder	
pt-PT	13/06/2021 00:40	File folder	
UPI	13/06/2021 00:40	File folder	
SkylumLuminarNFTBetaVersion.exe	12/06/2021 23:29	Application	791.202 KB

One of the first things you may notice is the large filesize of the so called beta version. As you've seen from before in Ariel's tweet, the filesize was 745MB, while this file is a whopping 791MB!

But why is this file so large and why does it matter?

- The attacker has appended their original file with a large chunk of *overlay* data; to put it simply - a bunch of extra data that does nothing.

- The attacker has increased the filesize this much to try and evade antivirus software and scanning tools; for example, a well-known service to scan suspicious files, [VirusTotal](#), only accepts files up to 650MB, while some antivirus scanners may not even scan a file this large.
- While you could upload the original RAR file; the attacker has password-protected it and VirusTotal will be unable to scan it properly. You could re-package it, but the file itself may not be scanned.

Having said all that, after removing the excessive overlay, a much more reasonable filesize is obtained: 175KB. This new file's properties are:

- MD5: d93de731781723b3bb43fa806c5da7d1
- SHA-1: 1d49e7d163bce8cc6591ea33984796c531893b47
- SHA-256:  
b9923cdcd07e3e490a729560aa6f7c9b153ac0359cc7fa212c65b08531575a5a
- Creation Time: 2021-06-12 20:46:31
- VirusTotal results:  
<https://www.virustotal.com/gui/file/b9923cdcd07e3e490a729560aa6f7c9b153ac0359cc7fa212c65b08531575a5a/detection>

Of note is the creation or compilation time: this is the date and time the file has originally been created. While this can be spoofed, I do not believe it is the case here. This time matches with when the attack appeared. It is however highly likely more files, such as the one in Ariel's tweet, do the round.

This file will then execute a new file; which is the RedLine infostealer malware. This file has the following properties:

- MD5: b7df882c1b75c753186eec8fcb878932
- SHA-1: a04339be16a3b48d06017f44db7e86b3c8982110
- SHA-256:  
2917305ac2959a98296578c46345691ccf638bdcc0559134432f5993da283faa
- Creation Time: 2042-10-31 08:29:02
- VirusTotal results:  
<https://www.virustotal.com/gui/file/2917305ac2959a98296578c46345691ccf638bdcc0559134432f5993da283faa/detection>

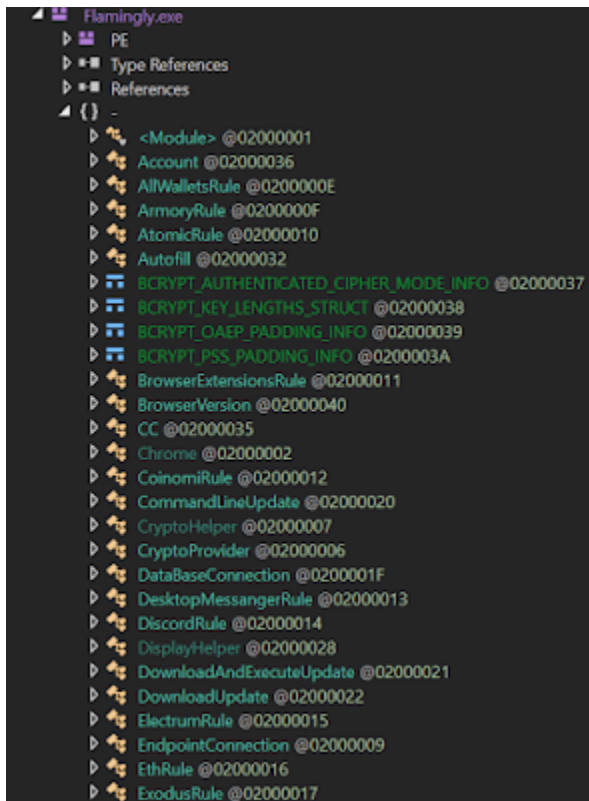
Note the creation time is different: set in 2042 - this is obviously faked by the attacker to reveal when exactly it has been created. However, with the above data, we can assume it was created in the last 5 days or so.

As mentioned before, once you execute the **SkylumLuminarNFTBetaVersion.exe** file, you will be infected with the RedLine infostealer malware. ProofPoint has reported on this malware first in March 2020: [New Redline Password Stealer Malware](#). This malware has

many capabilities, including, but not limited to:

- Steal username and password from browsers;
- Collect extensive system information;
- Execute commands, such as downloading and uploading other files, opening links and so on;
- Steal cryptowallet information - both from Chrome extensions as well as typical *wallet.dat* files. The extensions targeted are:
  - YoroWallet
  - Tronlink
  - NiftyWallet
  - Metamask (refer also to Nicole's tweet)
  - MathWallet
  - Coinbase
  - BinanceChain
  - BraveWallet
  - GuardaWallet
  - EqualWallet
  - JaxxxLiberty
  - BitAppWallet
- Steal data from other software, such as:
  - Steam;
  - Telegram;
  - FTP clients such as FileZilla.

The screenshot below displays part of RedLine's functionalities:



RedLine will first gather some basic information about your machine, such as the machine name, external IP address, your geography and so on. It gathers external information by querying one of the following IP lookup services:

- <https://api.ipify.org>
- <https://icanhazip.com>
- <https://wtfismyip.com/text>
- <http://bot.whatismyipaddress.com/>
- <http://checkip.dyndns.org>

Note these services are **not** malicious, they are simply being used by the attacker to gather more information. Interestingly enough, RedLine will use SOAP HTTP (POST) requests to its command and control server (the server or machine controlled by the attacker where your data will end up) using the following IP:

- **185.215.113.60;**
- On port 59472;
- This IP resides in the Seychelles.

Another domain and IP observed is (from ARC's tweet above, the files in that archive were almost 600MB):

- **xtfoarinat.xyz;**
- On IP 92.38.163.189;
- This IP also has [sinaryaror.xyz](http://sinaryaror.xyz) resolve to it, another RedLine command and control server.

One may also observe connections to tempuri.org. This is a default placeholder for web services, and is not atypical when using SOAP over HTTP. Tempuri is **not** malicious.

Finally, after receiving all this data, the attacker can start logging into your accounts, attempt to steal your tokens, impersonate you and so on. The attacker can also install other malware if they wish, such as ransomware.

## What now? Detection

---

### Good news:

---

The variant discussed in this blog does not appear to *persist*: in other words, after a reboot, its process will not be active anymore, at least for the variant discussed in this blog post.

### Bad news:

---

Everything else - unfortunately, RedLine works pretty fast and a few minutes are enough to exfiltrate all your data and for the attacker to fully compromise all your accounts.

Luckily for us, RedLine stealer *should* be detected by most commercial and free antivirus software products on the market. A few recommendations to get rid of the RedLine variant discussed in this blog post - note this may not fully cover the variant you encountered:

1. **Contact** your NFT provider, cryptowallet provider and so on as soon as possible via **telephone** call or **another computer** and inform them of what happened; ask for a temporary block of your account or to at least temporarily block any funds from now on.  
**>>> It is very important you do this first! <<<**
2. If you can, **change your credentials from another machine**; such as your phone, your partner's laptop, ... Note it's recommended to change your credentials at least for your email accounts and for your wallets - focus on the most important accounts first! If you do not have this possibility, continue with the steps below.
3. Open Task Manager, go to the **Details** tab and search for any process with the following names:
  1. SkylumLuminarNFTBetaVersion.exe;  
Flamingly.exe;  
FieldTemplateFactory.exe;  
PaintingPromoProject;  
*Alternatively, the name of the file you executed.*

2. Now, kill the process by right-clicking on it > select **End Process** (or **End Task**).

4. If you have a firewall or proxy, block the IPs **185.215.113.60** and **92.38.163.189**.

5. Run a scan with your currently installed antivirus **and** a scan with an alternative product, for example, Malwarebytes (has a free version);

1. You can also use Eset's Online Scanner (free):

<https://www.eset.com/int/home/online-scanner/>

6. Enable the Windows Firewall: <https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f>

1. While this might not have much impact at this point, it will give you an additional layer of protection from other threats;

7. **Delete** all the files you have previously downloaded if they still exist on your system; if you'd like me to analyse them, you may send me a copy first;

8. If the above scans have turned up:

**Clean:** have you executed the file?

1. If not, you are **not** infected.

2. If you did, and the scanners turn up with nothing, it's possible your current antivirus product has blocked the attack.

3. You might also want to Refresh your PC to have peace of mind.

**Not clean** (there were detections): let the above product (e.g. Malwarebytes or Eset) clean them up and reboot your computer.

- Finally, **reset all** (or the rest of) **your credentials**. Do this only when you know your machine is clean! Alternatively, reset your credentials from another machine as indicated earlier.

It's important to follow these steps as soon as possible to prevent any damages.



## Prevention

---

You've come this far, or perhaps you simply skipped to this part - arguably the most important one: **to prevent this attack from happening in the first place**. So how can this be achieved?

1. First and foremost: **ensure you are using Windows 8.1 or later**. Older Operating Systems, such as Windows 7, are no longer supported by Microsoft and have additional vulnerabilities attackers may exploit;
2. **Install an antivirus** and enable the Windows Firewall. **It does not matter if the antivirus is free or not**; paid versions do offer more features, but a free version will do just as much.
  1. Starting from Windows 10, Windows Defender should protect adequately from attacks such as the one described in this blog post. Other free alternatives are Kaspersky's free cloud antivirus and Malwarebytes.
  2. When you get any file, scan it with your antivirus first! (typically done by right-clicking on the file or folder)
  3. When in doubt, upload the file to VirusTotal. Note however the tactics used here: if there's a really large file, it may not be able to be scanned properly - this can be an indication of malicious intent!
3. **Set UAC (User Account Control) to the maximum level**: Always Notify - this will stop some additional attacks (you will get more prompts; if you do, take a pause and verify what's on the screen should indeed be executed). Here's how to do that:  
<https://www.digitalcitizen.life/how-change-user-account-control-uac-levels/>
4. **Enable file extensions**: some extensions, such as **.scr**, historically a *screensaver* file; are in fact executables - which could contain malicious code, as was the case in Ariel's tweet. Do **not** open or run these files. This will also protect you against the "double extensions" trick. A file named *commission.jpg.exe* will now be visible as such - if file extensions are disabled, you would see *commission.jpg* - see the difference? Here's how you can enable file extensions:  
  
<https://www.howtogeek.com/205086/beginner-how-to-make-windows-show-file-extensions/>
5. **Create unique passwords** where possible; if feasible; use a password manager;

6. **Enable MFA** (or 2FA if MFA is not available) on all your sensitive accounts; this will add an additional layer which is typically very hard for the attacker to guess or crack. Google "your service/ account + MFA" for specific instructions;
  
7. If you receive a new commission or request to create art, **stop and think first** - ask yourself these questions:
  1. Is this coming from a reputable account or from a totally new account?
    1. If reputable, can I verify their claim or request somehow?
    2. If from a new account: be extra wary!
    3. If from an account with very low followers/following: be extra wary!
  2. How will they pay me?
    1. Are they using a verified cryptowallet, or trying to set me up for something shady?
    2. Do they have any reviews on their (public) profile, if any?
  3. What are they asking of me exactly?
    1. Are they indeed sending just images, or is there an executable file or "special software" I am supposed to download/open?
  4. Where are their links or attachments leading to?
    1. Are these leading to another service, e.g. imgur.com, or something different altogether?
  5. I have downloaded the file(s), but I do not trust the source;
    1. Delete it or ask for more information;
    2. Block the sender if you are suspect and report their account, delete any files;
    3. You can double-check by scanning the files with your antivirus, or uploading it to VirusTotal. The same nuance as above applies however.
  6. You can also Google any information they send through to further verify their claims.
  
8. **Finally** and where possible;
  1. Use a hardware instead of software wallet;
  2. Secure your seed phrase; store it offline, for example, on an external drive or use pen and paper;
  3. Verify the security settings in your wallet or crypto provider: perform a check of which other security features you can enable, and enable them.

Manifold, a company that creates blockchain products for NFT communities, has also written an **excellent** post-mortem of this attack which includes additional advice - I highly recommend you to read it: <https://manifoldxyz.substack.com/p/the-fvckrender-hack-post-mortem>

## Conclusion and afterthoughts

---

It's not the first time a highly targeted or specific attack occurs on communities that use crypto in some form or another, for example, at the end of 2019, Monero's download site and binaries were compromised for a brief time.

If you have been targeted by this attack, and you have been compromised, follow the advice in this blog as soon as possible to clean it up and to prevent any future attack.

This attack was quite specific and targeted - there is really no need to feel bad if you have been affected, as it can happen to anyone. Explain to your crypto provider what happened, and they should be able to help you out.

I'd like to thank all the vigilant users on Twitter out there for creating awareness, and I hope this blog has provided further insight. If you were affected, and you'd like me to analyse any suspicious file, or would just like to comment, use the comment section below or contact me on Twitter. Refer to my About me page for even more contact details.