
[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)
> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)
> **Pixiv, DeviantArt artists hit by NFT job offers pushing malware**

Pixiv, DeviantArt artists hit by NFT job offers pushing malware

By
Bill Toulas
(<https://www.bleepingcomputer.com/author/bill-toulas/>)

May 4, 2022

02:46 PM

1



Image: Cyberpunk Ape Executives (<https://twitter.com/ApeExecutives>)

Users on Pixiv, DeviantArt, and other creator-oriented online platforms report receiving multiple messages from people claiming to be from the "Cyberpunk Ape Executives" NFT project, with the main goal to infect artists' devices with information-stealing malware.



"Cyberpunk Ape Executives" is a limited collection of non-fungible tokens (NFTs) following the closed-club approach that has given similar ventures astronomical fame and value.

As reported by Malwarebytes

(<https://blog.malwarebytes.com/scams/2022/05/fake-cyberpunk-ape-executives-target-artists-with-malware-laden-job-offer/>), threat actors are targeting artists with offers to work with the people behind the project and design a new set of characters to expand the collection with new NFTs, offering compensation of up to \$350 per day.

The message sent to the artists is given below:



"Hi! We appreciate your artwork! Cyberpunk Ape Executives is inviting 2D-artists (online / freelance) to collaborate in creating NFT project. As a 2D-artist you will create amazing and adorable NFT characters. Your characters will become an important part of our NFT universe! Our expectations from the candidate: 1) Experience as a 2D-artist 2) Experience and examples of creating characters 3) Photoshop skills."

"Main tasks: 1) Creating characters in our NFT style 2) Interaction with Art Team Lead on task setting, feedback. For further communication check out the examples of our NFT works: [url removed] and send a reply (CV + examples of your works) for this position. Approximate payment per day = \$200-\$350. We make payments to PayPal, BTC, ETH, LTC."

Cyberpunk ape malware

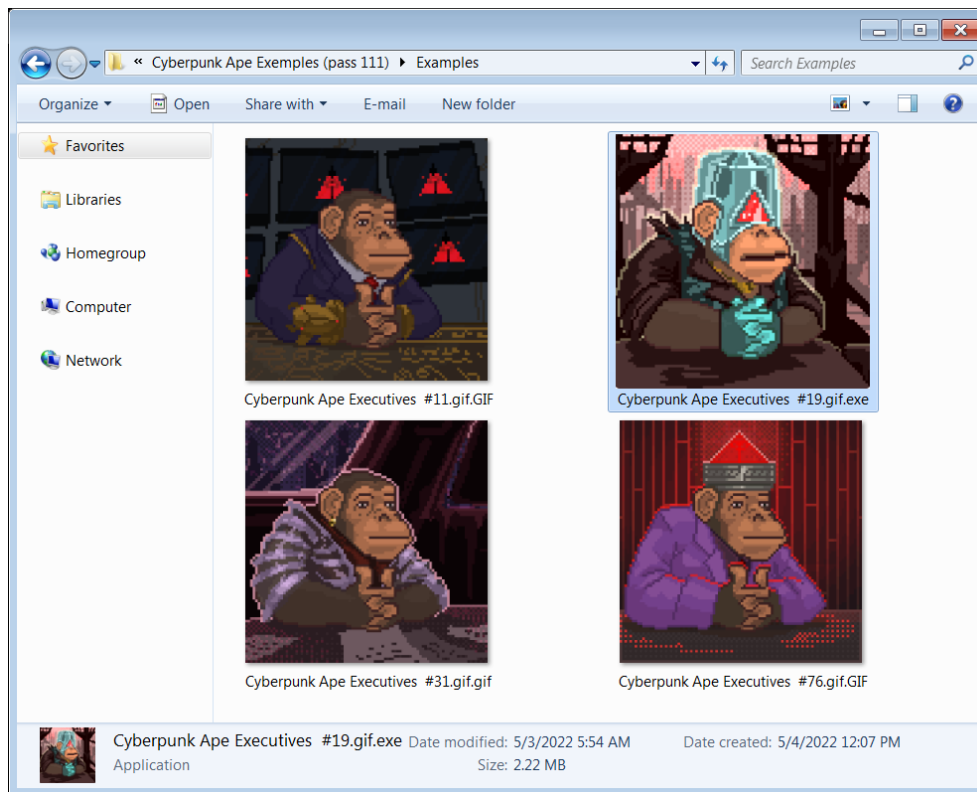
The messages sent to the artists contain a link that, if clicked, leads to a MEGA download page from where the victim can download a password-protected 4.1 MB RAR archive named 'Cyberpunk Ape Exemples (pass



111).rar' that contains samples of Cyberpunk Ape Executives artwork.

This is supposed to help the artists understand the style they should follow and create a false sense of legitimacy to the job offer.

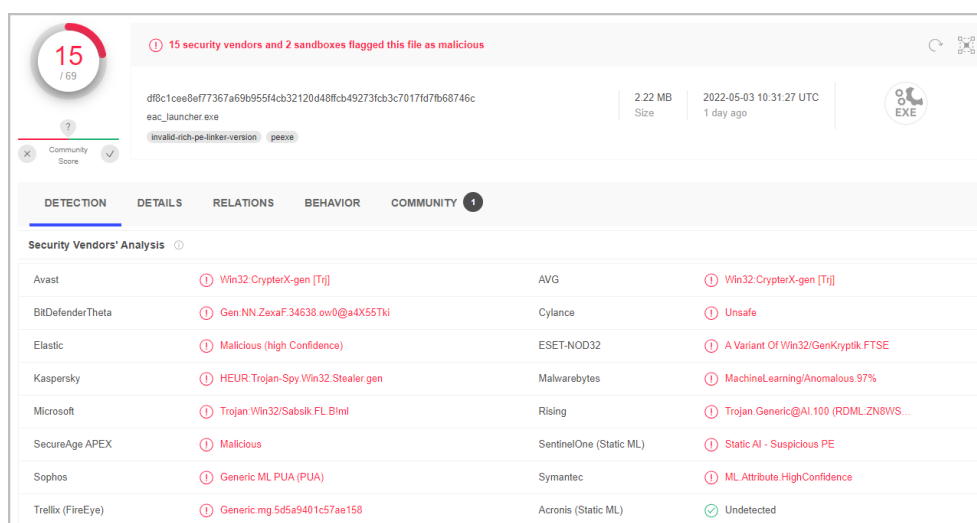
Inside the archive, the artists will find GIFs of Cyberpunk Ape Executives NFTs, and among them, an executable file made to look like another GIF image, easily blending in with the rest of the collection.



Executable disguised as an NFT GIF image

Source: Bleeping Computer

This executable is a malware installer that will infect the device with an information-stealing trojan with a good chance of bypassing AV detection based on current VirusTotal detections.



Virus Total check returning low detection chances

Source: Bleeping Computer



Info-stealers typically target information stored on web browsers, such as account passwords, cryptocurrency wallets, credit cards, or even files on the disk.

When the threat actors get their hands on the account credentials of a notable account with a high number of followers, they use that to promote the same scam to even more users.

This could be even more dangerous for artists who work with NFTs, as stealing victims' wallets will allow the threat actors to steal any cryptocurrency or NFTs stored within them.

Many creators report that bot accounts kept sending these messages every few minutes, while other artists say they received the message in Japanese.

How to stay safe

Job offers, especially the lucrative ones, can be enticing to the point of tricking people into jumping into immediate action, but you should never do that.

Instead, you should contact the project or company directly to confirm the email or review their Twitter accounts for further information.

Doing so would show that the Cyberpunk Ape Executives project warns users about this scam.

CYBERPUNK APE EXECUTIVES (PHASE ONE SOLD O... 
@ApeExecutives

There's currently a scam going around with people pretending to work with us. This is not real. Don't respond. Don't click the link. Report the people who are doing this on the platform they contact you on.
[#ApeExecutives](#)

