"Operation Chart Hunt": An Analysis of Data Theft Targeting NFT Artists

Antiy CERT

First draft completed: June 1, 2022

First published: June 2, 2022

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Since April this year, Antiy CERT has monitored multiple theft activities targeting non-fungible token (NFT) [1]C2 addresses and other features, they are linked to large-scale theft operations initiated by the same attack group. Since the attackers' main target is NFT artworks, Antiy named this activity "Operation Chart Hunt".

The attackers posed as employees of mobile game development company PlayMe Studio, NFT project "Cyberpunk Ape Executive", and other companies, sending job recruitment information through art creation social platforms such as ArtStation, Pixiv, and DeviantArt. Each attack message contained a link to a download page where victims could download a compressed file. The compressed file contained not only several sample images but also a stealing Trojan disguised as an image. By hiding the extension, it could easily be mistaken for an image and executed upon click.

Once executed, the stealing Trojan automatically collects computer system information, browser data, e-wallets, NFT managers, password managers, and other software data, then encrypts and transmits this data back to the attacker's server. If social media platform accounts and passwords are stored in the browser, the attackers will also use the stolen information to log in to the social media platform and continue to post phishing messages to users on other platforms, further expanding the scope of victims. This attack campaign has been ongoing for over a month. During this period, the attackers have continuously changed their shell protection technology while retaining the core functional payload to evade detection by antivirus engines and security software.

With the rise of the next-generation internet "metaverse," the market for NFTs—identity symbols within the metaverse—has also seen rapid growth. However, as NFTs gain wider recognition, they have also become a new

target for attackers. NFTs are a relatively new type of digital asset. Similar to mainstream digital assets like Ether (ETH) and Bitcoin (BTC), they are stored as data on the blockchain and in NFT-compatible wallets. Therefore, attackers can steal the account and password stored in cryptocurrency wallet clients or browsers to open a victim's digital wallet and steal the NFT artworks. Furthermore, attackers can steal user accounts and passwords through forged phishing websites or attacks on NFT trading platforms. Because NFTs utilize digital technologies such as blockchain, once stolen, there is currently no way to recover them other than immediately locking and prohibiting trading.

Antiy CERT continues to follow up and analyze such incidents. It has been verified that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and eliminate this stealing Trojan.

2 ATT&CK Mapping Diagram Corresponding to the Incident

The distribution of technical features corresponding to this event is as follows:

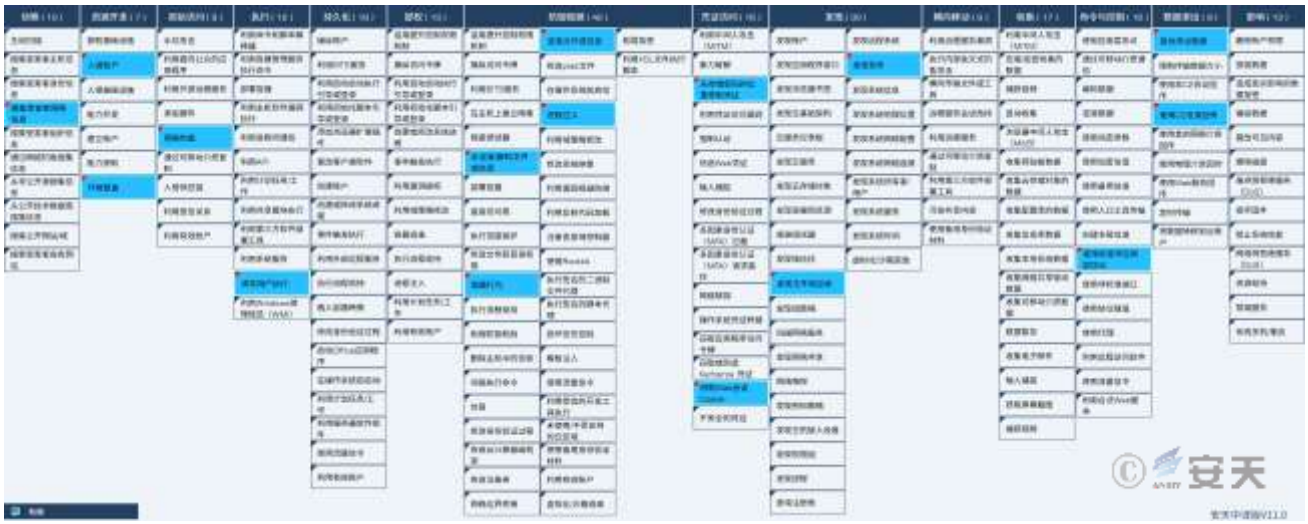

Figure 21flowchart2payload and Shellcode3malicious payload injected into RegSvcs.exe4data5

3 Summarize

In recent years, NFT transaction volume has steadily increased, and the NFT market has become increasingly popular. However, NFTs are still in their early stages of development, and many issues remain to be addressed. For example, due to the use of digital technologies such as blockchain, once an NFT is stolen, there is currently no way

to recover it other than immediately locking and prohibiting trading. In fact, NFT holders are increasingly being targeted by attackers, and users should remain vigilant to avoid negligence that could allow criminals to exploit them.

Recent changes in the samples used by the attackers indicate they are employing various packer protection techniques to evade detection by antivirus engines and security software. Furthermore, the attackers are using stolen accounts and passwords to log into social media platforms and continue to distribute phishing messages to users on other platforms, thereby expanding their reach. This suggests that this theft activity will continue for some time to come. Users should remain vigilant against such attacks and avoid opening unidentified web links or downloading and executing suspicious files to avoid potential loss of digital assets.

Antiy CERT continues to follow up and analyze such incidents, focusing on the technical changes and characteristics of stealing Trojans, proposing corresponding solutions, and deploying corresponding defense capabilities into security products. Antiy IEP not only provides basic functions such as virus detection and active defense, but also provides enhanced capabilities such as terminal control and network control, which can effectively defend against such threats and ensure the security of user data.

4 IoCs

9B472A7F4E7B7DE1D5CE9049F400EFBB
D2233AA3AC1490968F62A9C9D55E9D36
A592073C9AA063756605EF0EAF0AC289
BDD239862D7F615C5EB709EF5C5E282F
EF47843068F3005F3ACD454C9BEE744F
02D9EEE4BE3E1A41037222E3F43662AB
667710059ECCD9C23880AACDFD0DB5ED
260F44E2632DDA4C511F3B4DFEB58AD8
FD4B860F4504C6A92B80E42AFA8BD525
1A08486FDF53F0F6A1A2781045570E73
CD5E45337B22986033EBE4553C242FAF
70161EB7087936D92D9762A8A5F99FF1
01C77CDD4DB48A2FDB976A8D79343D5C
75D03DE5C50EA9E54654A229CFBC5827

3CAEEB9E025BFFF2215D84CD25E26187
DA0F3222B92E10A24546FA7B266F2A0B
F1F83A9CE9A0227DDBC8FBF31B16589B
A818170717263831D6E42AC54DD07183
9A3439E9A4DC5962C9EC4411BD30AB16
E05E73FB5D9DF18317DA096C65F5554E
4330BDA7F122DBC0A4917AE48A4F3457
FC1982DB2F536F0D4B7C2B50E4A385A1
ADB3E6C596FC36B8D89AFFE0CE68614E
498E68AC36E7A7CA8BF032E3549861E9
AC74EA4EE583202166C1EED9A5381A9A
61EB4ABCB5D7224EA7A17AB24A628EAC
674543B35C33EE2343E09F1672F90F3C
C9403AC2AEEB66BDDBD5D181B84D61F5
5D5A9401C57AE158076D8FAB2418B174
93BB6CC0EF8C7FB729B0BF0D67C96989
154182A094041880D0757B65804FE6CC
50EE952A73A2612084D266D46E59F9D6
22BF1AABA120FD55BA1D9C3D316DBF30
41AE1344A5D3BB23117A81047A593BD2
8925177864A9112A42B3117750C07781
CF997C7D4BB2023A28AFB81BC5B43529
F0DF194AC8E5100B9C05A8B7C97CF634
81A966F3211871E76BE12C05279C23AD
035B2F18376C3067F7789160C2A9EBD4
C4FFCDF45DBFF50DAC01947063B8D4FE
4773C61E1AF41892874B559C9A6F597F
45.142.122.179:7777

Appendix 1: References

[1] NFT (Non-Fungible Token)

https://baike.baidu.com/item/NFT/56358612

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and

services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.

