NFT Lure Used to Distribute BitRAT

fortinet.com/blog/threat-research/nft-lure-used-to-distribute-bitrat

February 14, 2022

Despite being around for many years, blockchain captured the zeitgeist of the digital movement with the advent of Bitcoin. Digital currencies, however, are not the only application of this technology. Non-fungible tokens (NFT) entered the popular lexicon in 2021. An NFT is a digital token that uses blockchain to verify the authenticity of digital content and ownership, such as art, music, collectibles, and in-video-game items.

The first major NFT splash came in March 2021, when the digital work of art “Everydays – The First 5000 Days” created by the digital artist “Beeple” was auctioned and sold for a record-breaking $69 million. Later that month, the NFT of the very first tweet posted by then-Twitter CEO Jack Dorsey was sold for $2.9 million. NFTs even gave new life to a popular 10-year-old internet meme, “Nyan Cat.” The original creator remastered the GIF and sold it as an NFT for 10 Ethereum ($590,000).

Exclusive possession of unique assets tends to drive the desire for ownership—and the price—sky-high. And predictably, online criminals are there trying to exploit this activity.

FortiGuard Labs recently came across a peculiar-looking Excel spreadsheet that seemingly included NFT-related information. But instead, it downloads and installs the BitRAT malware in the background. This blog describes how this attack works.

Affected Platforms: Windows
Impacted Users: Windows users
Impact: Compromised machines are under the control of the threat actor
Severity Level: Medium

Strange looking Excel macro file (XLSM) and target

The original source of the malicious Excel file has not been identified. However, the file provides some clues as to its origin and target. First, the XLSM is named “NFT_Items.xlsm”. Second, the file has two workbooks, one of which is in Hebrew. That workbook contains what appears to be legitimate Discord rooms that deal with NFTs. It also includes the names of NFTs, forecasts for potential investment returns (hyped, solid, and 50/50), and selling quantities. Finally, like many similar recent attacks, this attack abuses Discord by using it to host malicious files. These points provide enough evidence to conclude that the attacker likely sent a message to NFT enthusiasts in Israel to entice them to download and open the malicious XLSM.

Figure 1. Malicious XLSM file, “NFT_Item.xlsm”

The XLSM contains a malicious macro, which the user is asked to enable upon opening the file. Once the XLSM file is opened, and the macro is enabled, the XLSM drops a batch file. It then uses a PowerShell script to download another file from Discord, NFTEXE.exe.

Figure 2. Malicious macro in NFT_Item.xlsx

Figure 3. Windows batch file dropped by the malicious macro in NFT_Item.xlsx

Figure 4. Decoded PowerShell script delivered by the batch file in Figure 3

The downloaded NFTEXE.exe is a .NET executable file that attempts to run "ipconfig /renew" and then pull down yet another file, NFTEXE.png, from Discord. Disguised as an image file, NFTEXE.png is pure data with all its strings flipped (see *Figure 5.*).

Figure 5. Reversed strings in NFTEXE.png

Running "ipconfig/renew" is an attempt to disrupt analysis of the malware should it find itself running in a cloud environment by dropping the connection to the analyst so that the NFTEXE.png will not be downloaded.

NFTEXE.exe then reverses these strings into the next stage file, “Nnkngxzwxiuztittiqgz.dll”. A .NET DLL appears to have been compiled on January 2nd, 2022. Since the malicious XLSM was made available on a public online scan service on January 3rd, the XLSM file was distributed soon after compilation.

NFTEXE.exe copies itself as C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Adobe\Cloud.exe, which runs at every startup to maintain persistence. NFTEXE.exe also makes a copy of MSBuild.exe, a legitimate Windows file, to C:\Users\[username]\AppData\Local and runs it. NFTEXE.exe then injects a malicious payload into the running MSBuild.exe using Nnkngxzwxiuztittiqgz.dll.

BitRAT

Our analysis determined that the payload is BitRAT, a Remote Access Trojan (RAT) that was first sold in a hacking forum in August 2020.

One trait of the BitRAT sample that FortiGuard Labs analyzed is its usage of Hidden VNC (HVNC). HVNC provides an attacker with remote access to the compromised machine. BitRAT is known to have borrowed the HVNC code from another malware, TinyNuke, the source code of which was leaked in 2017. Another notable thing included in the BitRAT sample is a string, “AVE_MARIA”, used as a traffic header value when an HVNC client communicates to its C2 server for verification. The HVNC communication is designed to fail if the traffic header value is not “AVE_MARIA”.

More BitRAT functionality was revealed during our analysis once additional strings were decrypted. For example, we were able to see that BitRAT can bypass User Account Control (UAC)—a Windows security feature first introduced in Windows Vista that helps prevent unauthorized changes to the operating system —and Windows Defender— an anti-malware component of Microsoft Windows first released with Windows XP. We also found that this variant can also monitor the screen and, if present, utilize the webcam.

Figure 6. More BitRAT capabilities

After the strings were decrypted, it also became apparent that BitRAT uses Slowloris for its DDoS capabilities.

Figure 7. Slowloris DDOS

Other BitRAT functionality includes:

- Stealing credentials from browsers and applications installed on the compromised machine
- Mining Monero cryptocurrency
- Logging keystrokes
- Uploading and downloading additional files to the compromised machine
- Listening live through a microphone

In an attempt to hide stolen information, this variant of BitRAT stores collected data (keystrokes, clipboard data, etc.) in an alternate data stream (ADS) file that is majority encoded in Base64.

Figure 8. BitRAT writing to ADS file C:\Users\REM\AppData\Local:11-01-22

As can be inferred by the file name above, a new file will be created each day and given the name of the current date.

Figure 9. Contents of the ADS log file.

The C2 server (205[.]185[.]118[.]52) this particular BitRAT variant connects to belongs to FranTech Solutions, a hosting provider that is known as a bulletproof hosting service provider. A bulletproof hosting service is just like a regular web hosting service in that they are used to store content. The difference is that a bulletproof hosting service also hosts illegal content, such as malware, C2, exploit kits, and fake shopping sites. They also tend to be more resistant to complaints and takedown requests.

Conclusion

In this attack, NFT was used to lure a victim into opening a malicious XLSM file to deliver BitRAT, which put the victim’s data and machine at risk.

NFT is a new internet phenomenon that some view as a legitimate investment and money-making opportunity. Any investment comes with risk, but certain risks taken before money changes hands are avoidable. Be mindful that attackers often use attractive and trendy subjects as lures. As NFTs become increasingly popular, they will be used to entice victims into opening malicious files or clicking on malicious links. Standard security practices such as not opening files downloaded from untrusted or suspicious sources can prevent threat actors from gaining access to users' money and valuable data.

Fortinet Protections

The FortiGuard Antivirus Service detects and blocks this threat as MSIL/Agent.JWX!tr.dldr and VBA/Agent.XC!tr.

FortiEDR detects the downloaded NFTEXE.exe as malicious based on its behavior.

All network IOCs are blocked by the WebFiltering client.

IOCs

Sample SHA-256:

- 88ef347ad571f74cf1a450d5dad85a097bb29ab9b416357501cdc4c00388f796
- 342a5102bc7eedb62d5192f7142ccc7413dc825a3703e818cf32094638ebd17a

Network IOCs:

- hxxps://cdn[.]discordapp.com/attachments/923977279179202600/927289948825079828/NFT_LIST.xlsm
- hxxps://cdn[.]discordapp.com/attachments/927290851930013766/927291495604699167/NFT_LIST.xlsm
- hxxps://cdn[.]discordapp.com/attachments/923858595353874472/928279600659234826/NFTEXE.EXE
- 205[.]185[.]118[.]52

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.