What is Clipper Malware? How does it affect Android users?

On January 8, 2019, users saw the first version of Clipper malware on Google Play Store. It has disguised as a harmless application to trick all downloads, then start redirecting electronic money to the owner of the malware.

On January 8, 2019, users saw the first version of Clipper malware on Google Play Store. It has disguised as a harmless application to trick all downloads, then start redirecting electronic money to the owner of the malware.

But what is Clipper malware, how does it work and how can it be avoided from this malware?

Learn about Clipper malware

1. What is Clipper malware?
2. How Clipper works
3. How long has Clipper existed?
4. Which applications contain Clipper?
5. The increase in electronic money attacks
6. How to avoid an attack from Clipper?

What is Clipper malware?

Clipper targets e-wallet addresses in a transaction. This wallet address is like the pre-electronic version of the bank account number. If you want someone to pay you electronically, you must provide them with your wallet address and the payer enters it into their payment details.

Clipper hijacks e-money transactions by swapping addresses for real addresses with Clipper's wallet. When users make payments from an electronic money account, they will pay the author of Clipper instead of the original intended recipient.

This can cause some serious financial losses if malware manages and appropriates a high-value transaction.

How Clipper works

Clipper does this swap by tracking the clipboard (where the copied data is stored) of a device infected with Clipper. Every time a user copies data, Clipper checks whether the clipboard contains any e-wallet addresses. If so, Clipper will swap it with the address of the creator of the malware.

Now, when users paste the address, they will paste the address of the attacker instead of the legal address.

Clipper exploits the complex nature of wallet addresses. These are long strings of numbers and letters that seem to be randomly chosen. It is unlikely that the payee will recognize the address that has been swapped, unless they have used this wallet address many times.

Even worse, its complexity makes users tend to copy and paste addresses more than manually typing with the keyboard. This is exactly what Clipper wants!

How long has Clipper existed?

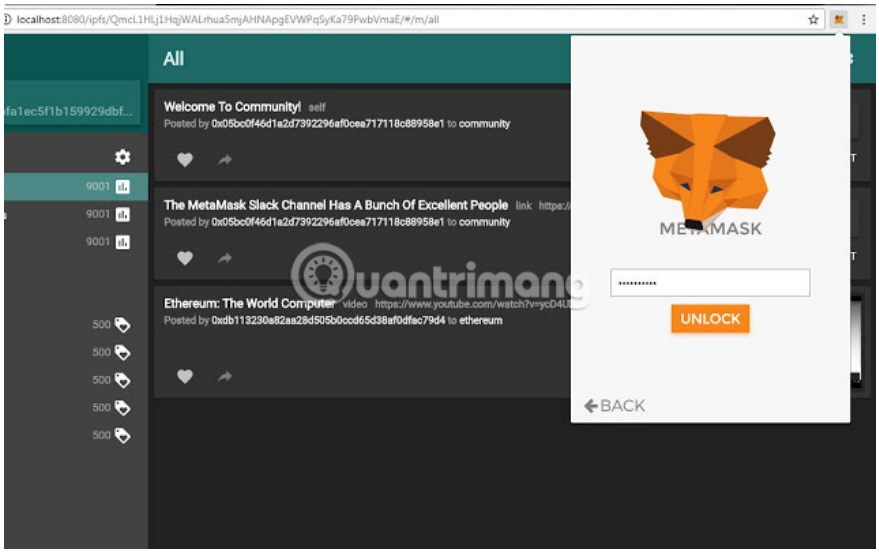
Clipper itself is nothing new. It appeared around 2017 and mainly focused on Windows computers. Since then, Clipper aimed at Android has been developed and sold on the black market. Infected applications can be found on shady sites.

Such sites are the foundation for the 2016 Gooligan malware, which has infected over 1 million devices.

This is the first version of the application on Google Play Store, officially infected with Clipper. Successfully downloading malware-infected applications to the official app store is a desirable scenario for malware distributors. The App downloaded from the Google Play Store provides a certain sense of security, making it more reliable than the apps found on a random website.

This means that people often download and install apps from here without a doubt, that's exactly what the creators of the malware want.

Which applications contain Clipper?



Clipper is in an application called MetaMask. It is a real service that allows browser-based distributed applications for Ethereum electronic money. MetaMask does not yet have an official Android application, so malware creators have taken advantage of this to make people think that the official version has been released.

This fake MetaMask application has done more than exchanging electronic money addresses in the clipboard. It also requires the user's Ethereum account details as part of a fake account setup. Once the user has entered the details, the malware creator will have all the information they need to log into the account.

Fortunately, a security company discovered Clipper before it caused too much damage. The fake MetaMask application was uploaded on February 1, 2019, but was reported and removed just over a week later.

The increase in electronic money attacks

Although this type of attack is quite new, it is not too surprising. Electronic money is a huge business now, and with it comes the potential to earn huge sums of money. While most people are satisfied with making money through legal means, there will always be those who choose to exploit illicit money from others.

Electronic money is the favorite target of malware makers worldwide. They take control of the processor on the device, turning it into electronic money for them without being detected by the main user.

Like this example of Clipper malware, security companies have found those who want to exploit illegal electronic money to infect malware on applications on Google Play Store. Thus, this may be just the beginning of electronic money-based malware that attacks users on Android phones.

How to avoid an attack from Clipper?

This sounds very scary, but avoiding an attack from Clipper is quite simple. Clipper depends on whether the user is ignorant of its existence and ignores the warning signs. Understanding how Clipper works is important to defeat it. By reading this article, you have completed 90% of the job!

First, always make sure you download the app from Google Play Store. Although Google Play is not perfect, it is much safer than other Internet shady sites. Try to avoid websites that act as a third-party app store for Android, as these sites are more likely to contain malware than Google Play.

When downloading apps on Google Play, double-check the total number of app downloads before installing. If an application has existed for a long time and has a low number of downloads, the download may be at risk. Similarly, if the application claims it is a mobile version of a popular service, check the developer name carefully.

If another name (even slightly different) from the official developer name, it is an important warning sign that something is not right.

Even if the phone is infected with Clipper, users can avoid an attack by being more cautious. Carefully check every wallet address that will be pasted to make sure it is not changed midway. If the address you paste is different from the copied address, that means Clipper is hiding on the system.

Perform full Android virus scans and delete any recently installed shady applications.

Clipper can harm anyone who handles large amounts of electronic money. The complex nature of wallet addresses, combined with typical user copy and paste trends, gives Clipper an opportunity to attack.

Many people may not even realize what they did until it was too late!

Fortunately, beating Clipper malware is simple: Never download suspicious applications and double check all wallet links before confirming the transaction.