Detecting a new type of malware that steals Windows passwords, installs a virtual currency mining tool and continues to spread trojans

A newly discovered malicious code will reach victims through ads displayed in search results. After successfully reaching the Windows computer, it will steal passwords, install cryptocurrency miners and run other trojan delivery tasks.

The malicious code called MosaicLoader is capable of installing Bitcoin miners and spreading malicious code.

Security software firm Bitdefender revealed that malicious code developed specifically for the Windows operating system called MosaicLoader will try to infect as many victims as possible. Unlike many viruses that spread through phishing attacks or unpatched software, MosaicLoader is a virus that is even advertised to potential victims.

The workstations can be threatened if unfortunately for MosaicLoader to get in and continue to spread other malicious code. One of them is Gupteba, a malicious code capable of developing backdoor systems to collect sensitive information, including passwords, usernames or financial information.

When users search for cracked versions of software, links to malicious websites show up at the top of the search results page. Because of the automated processes that trigger to buy and display ads, not everyone knows that ads are endangering users except for attackers.

People who work from home are more likely to download malicious code than people who work in offices.

According to Bitdefender, people who work from home are more likely to download pirated software than people who work in the office. Although anti-virus software can prevent malicious code, to comply with the installation regulations, many users who download illegal software are forced to turn off system protection when installing software.

Many crack (jailbreak) applications will mimic the metadata of real software files to make the software download and installation look the most professional and reliable. However, the danger behind that is something not everyone knows.

After downloading and installing the malicious software MosaicLoader, it will allow the attacker to access the victim's PC. Attackers can obtain usernames and passwords of online accounts, the researchers warn. The presence of additional malicious code on the compromised Windows computer shows that the main goal of the attacker is to steal information.

Users should be careful when following the advice of disabling anti-virus software because this can lead to the installation of malicious software, potentially at risk of remote system intrusion.