Mass Logger: Keylogger is extremely dangerous with the ability to change the world of malicious code

Mass Logger regularly updates and adds new features to avoid detection.

Security researchers at Cofense Intelligence have discovered and are closely monitoring a new keylogger called "Mass Logger". According to the researchers, Mass Logger can have an impact on changing the world of malware.

A keylogger is usually a small piece of software - or sometimes more dangerous, even a hardware device - with the ability to record every keystroke the user has pressed on the keyboard. Summing up the results of these keystrokes, the keylogger installer can obtain personal messages, email content, credit card numbers and of course the most dangerous of all types of user passwords.

According to calculations, keylogger is most used in phishing campaigns, malicious attacks. Currently, keyloggers are continuing to develop in terms of both the popularity and sophistication of the source code.

Cofense Intelligence is especially interested in Mass Logger because it is updated very quickly. The person behind Mass Logger is constantly updating and improving so that it easily bypasses security systems. With this ultra-fast development capability, Mass Logger authors can also quickly edit and add new features as required and customer feedback.

NYANxCAT is the author of Mass Logger. In addition, this object is also the owner of some other notorious malicious codes such as LimeRAT, AsyncRAT . Malicious, NYANxCAT hacking software is often rich in features and easy to use. However, Mass Logger may be the most advanced feature of NYANxCAT. For

example, Mass Logger has the ability to spread, install onto victim's computer via USB.

NYANxCAT is constantly improving the functions of the Mass Logger through updates. In just the last 3 weeks, 13 updates have been released by NYANxCAT. In the updated notes collected by Cofense, NYANxCAT revealed that new targets have been added to Mass Logger's identity theft function. In addition, a number of security measures have been added to prevent this keylogger from being detected by the antivirus system.

The variety of features and sophisticated evasion capabilities help Mass Logger stand out from other malicious code. For example, Mass Logger allows hackers to search for files in a specific format and copy them. Cofense found evidence that cybercriminals are abandoning other popular keyloggers like Agent Tesla to Mass Logger.

To combat Mass Logger and similar threats, Cofense recommends that system administrators be aware of suspicious FTP file transfer protocols or emails. Besides, users should not let strangers come into contact with their computer, do not click unreliable links.