

Detecting new malicious code capable of 'evading' most anti-virus software

Cybersecurity experts at HP company (USA) have discovered a new malware that is able to evade most anti-virus software. The new malicious code is named RATDispenser.

Specifically, security experts have discovered a new JavaScript downloader that distributes 8 remote access (RAT) [Trojans](#), keyloggers and information stealers. different. The special thing is that this new malicious code uses a number of techniques to be able to bypass the detection of most security tools, so it is very dangerous.



HP analyst Patrick Schlapfer said the new malware successfully infiltrated many of the victim's workstations because the anti-virus system detected only 11% of the [malicious code](#).

RATs and keyloggers help hackers gain access to infected computers through 'backdoors'. They will then use the access to steal user account credentials, cryptocurrency wallets, etc.

When a user opens an email containing malicious code in [JavaScript](#), a VBScript file is written and downloaded to the malware, before deleting itself.

Experts have detected at least three different RATDispenser variants in the past three months with a total of 155 newly discovered malware samples. This suggests that the malware may still be in development.

The researchers suggest that the author of the RATDispenser malware may be operating in the form of a malware business.

You finished reading the article "**Detecting new malicious code capable of 'evading' most anti-virus software**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

