New hacker tricks, increasingly more sophisticated, to avoid being exposed

Recently, security firm Fortinet (USA) has released a report on cyber security threats. According to this report, cybercriminals are becoming more and more sophisticated in cloaking and anti-analysis activities to avoid being exposed.

Recently, security firm Fortinet (USA) has released a report on cyber security threats. According to this report, cybercriminals are becoming more and more sophisticated in cloaking and anti-analysis activities to avoid being exposed.

For example, Fortinet found that hackers using impersonating e-mail with an Excel attachment contained a program running inside a malicious file (macro) during a spam distribution campaign. This macro has the ability to disable security tools, cause memory problems, execute arbitrary commands. The special thing is that it is designed to run only on Japanese systems. This procedure makes it difficult for normal network security measures to detect malicious code.

Photo: CPO Magazine.

Another example is a variant of the Dridex malware. Every time the victim logs in, this malicious code has the ability to constantly change the names and hash functions of the files. This makes it difficult to detect malicious code on infected server systems.

Similarly, Zegost malware uses sophisticated technology to erase all archives of operational history and run below the radar control. Hackers even put orders to keep this malicious information from staging and only start to carry out the infection when February 14, 2019, prevented the security tools from transmitting. appear now.

Meanwhile, instead of mass attacks, profiteering speculation, spyware and extortion are now turning to clear-targeted attacks, targeting specific companies and organizations. for ransom. Hackers have carefully studied the target, looking for security holes before deploying attacks to be able to execute arbitrary code without any interaction from the user.

According to Fortinet, extortion software is still a serious threat to companies, so it is necessary to prioritize patch development and improve awareness of information security. In addition, hackers can take advantage of the security holes of the remote computer control protocol (RDP) to spread malicious ransom.

According to the security firm, in order to protect itself from ever-growing cyber security threats, companies need to develop appropriate plans and implement integrated security solutions.

1. Hackers claim to be able to 'shutdown' 25,000 cars in just one note