Hackers are using new Microsoft Office vulnerabilities to distribute malware

Hackers are exploiting vulnerabilities in Microsoft Office software to spread a kind of sophisticated malware capable of stealing certificates, exploiting cryptocurrency and conducting denial of service (DDoS) attacks.

Hackers are exploiting vulnerabilities in Microsoft Office software to spread a kind of sophisticated malware capable of stealing certificates, exploiting digital money and conducting denial of service (DDoS) attacks. .

Researchers at FireEye have observed a new campaign to spread malware via spam to targets in the telecommunications, insurance and financial services industries and discover new attacks to exploit New vulnerabilities were discovered in Microsoft Office office suite.

Sophisticated designed phishing emails that relate to the selected target and include a ZIP file containing malicious documents, the user is encouraged to open it. Once these Microsoft Office related document files are accessed, Office vulnerabilities are exploited and PowerShell-based malware is run, infecting the victim computer.

One of the vulnerabilities exploited by attackers is CVE-2017-11882. Security vulnerabilities in Microsoft Office allow this code to run arbitrarily when a malicious file is opened. In this attack, the vulnerability allows additional downloads after activation using a malicious file attachment URL. The download file contains an extremely dangerous PowerShell script.

This attack also attempts to exploit CVE-2017-8759, a vulnerability that exists when Microsoft .NET Framework processes unreliable data and may allow an attacker to control an infected system. . In this case, the DOC file attached to the phishing email contains an embedded OLE object that activates the downloaded URL to start the PowerShell process. The vulnerability was revealed and patched in September 2017.

If the PowerShell script is run successfully, it will load the downloaded code from the server that controls and executes the malicious command, automatically extract the malware to the target computer along with the functions that allow the attacker Use Tor to hide traces. Malware also contains various plugins that allow an attacker to secretly access most types of data stored on the computer.

In addition, an attacker has the ability to steal passwords from popular web browsers, steal passwords from FTP applications and steal passwords from other email accounts linked in the computer.

Malware can also steal from secret e-wallets and steal license keys from more than 200 popular software applications, including Office, SQL Server, Adobe and Nero.

In addition to being able to steal information from a malicious computer, attackers can also assign infected machines to a larger computer network to help implement DDoS attacks and can use the machines. Calculated as a tool for digital currency mining.

Users should make sure that they have downloaded all the published patches for CVE-2017-11882 and CVE-2017-8759 vulnerabilities.

A Microsoft spokesperson told ZDNet: *"The security update was released last year and customers have applied them, or have enabled automatic updates to be protected."*

See more:

1. What is the Microsoft Office Upload Center? How to disable this tool?
2. Instructions for installing and using Office 2016
3. How to install Vietnamese language interface on Microsoft Office 2016