Phishing attack: The most common techniques used to attack your PC

Phishing attack is probably a term that is not unfamiliar to most internet users. In fact, it is also one of the most common forms of cyberattacks.

Phishing attack aims to carry out malicious activities to steal sensitive information such as usernames, passwords and credit card details by impersonating a trusted entity in a transaction. electronic, mainly via the internet.

Common techniques for phishing attacks

Macros Office

In phishing attacks, In general, creating malicious Office macros is still the most common attack technique commonly deployed by cybercriminals to infiltrate a PC after successfully deceiving the victim of opening a phishing email.

Phishing emails are the first stage in the majority of computer or intranet attacks. In particular, cybercriminals will use psychological tricks to persuade potential victims to open and interact with malicious emails (attach links or executables containing malicious code). This technique can include creating disguised emails, claiming to be from famous brands, fake invoices, or even emails sent from your partners or colleagues.

There are many methods that cybercriminals can exploit to use phishing emails to gain access to the systems they want. According to the results of researchers at cybersecurity firm Proofpoint, Office macros are the most popular technique for hackers to achieve this.

Macros are a function of Microsoft Office that allows users to trigger automated commands to perform a variety of tasks. However, this feature is also frequently abused by cyber criminals to break into computers. Since macros are usually enabled by default to run commands, they can also be exploited to execute malicious code and thereby inadvertently become a bridge to help hackers gain access and control over the victim's PC. .

Most attacks of this type will incorporate social techniques to encourage victims to turn on malicious macros by claiming that it is a necessary function for viewing Microsoft Word or Microsoft Excel attachments. Overall, this is a highly effective attack method for cybercriminals, with Office macros accounting for almost a tenth of all recorded cyber attacks.

Sandbox dodged

However, Office macros are not the only attack technique that cybercriminals use to perform highly effective phishing attacks.

Sandbox evasion is the second most common attack technique commonly used by hackers spreading phishing emails.

This is when malware developers build threat detection that can prevent the malware from working - leaving themselves effectively - when in suspicion that there is security software running on the machine. virtual or notice the emergence of 'defensive shields' established by security researchers. In general, the main purpose here is to prevent analysts from being able to test the attack - and to make the malware effectively hidden.

PowerShell

In addition, PowerShell is also frequently abused by attackers as a means of gaining access to networks after gaining initial foothold thanks to a phishing email. Unlike macro-related attacks, these attacks usually rely on sending and convincing victims to click on a link containing the malicious code to execute PowerShell. Such attacks are often difficult to detect because they are using a legitimate Windows function. That is also why PowerShell is still popular with attackers.

Another popular attack technique commonly used in phishing attacks involves redirecting users to websites containing malicious HTML code, then dropping the malware onto the victim's PC as they do. access. In addition, attackers can also hijack known email threads, contacts, and abuse a victim's trust for malicious purposes, such as sending malware or requesting information. login message.