Hacker exploited three vulnerabilities in Microsoft Office to spread Zyklon malware

Security researchers have discovered a botnet spread of malware through at least three new vulnerabilities published in Microsoft Office.

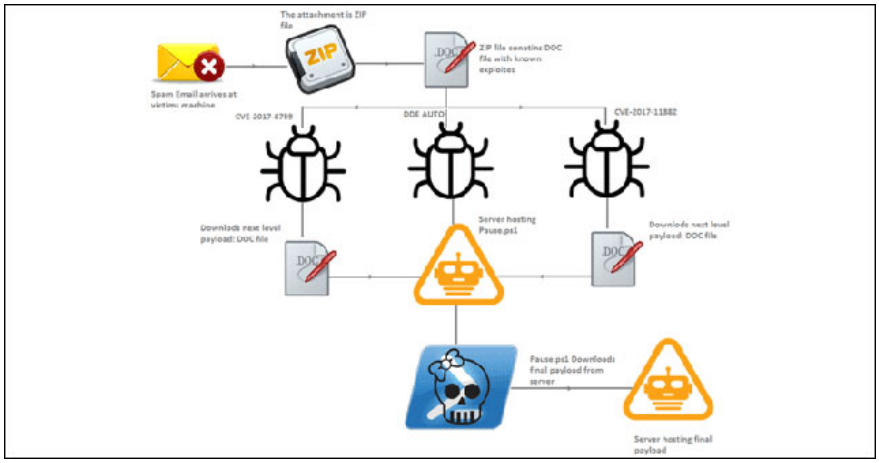
Security researchers have discovered a botnet spread of malware through at least three new vulnerabilities published in Microsoft Office. Named Zyklon, this malware is exposed after almost 2 years and is primarily targeted at finance, insurance and telecommunications companies.

What is a botnet, who does it use to attack, and how can you prevent botnet?

Starting operations in 2016, Zyklon is the HTTP botnet malware that communicates with the C&C server through the Tor anonymous network and allows an attacker to steal keylogs, sensitive information such as browser passwords or emails. It can also install plugins, silently use a poisoning machine for DDoS attacks or dig virtual money.

Zyklon versions are advertised in the underground market for $ 75 (regular edition) and $ 125 (Tor version). According to a recent study by FireEye, the attacker after the campaign uses **three Microsoft Office vulnerabilities** to execute the PowerShell script and download the payload from the C&C server to the victim's computer.

1. **.NET Framework RCE Vulnerability (CVE-2017-8759)** : the vulnerability executes remote code when Microsoft .NET Framework handles unreliable inputs. Attackers trick victims into opening files with malicious code via email and take control of the system. Microsoft has released this patch from the September update.
2. **Microsoft Office REC Vulnerability (CVE-2017-11882)** : memory interruption existed 17 years ago and was patched by Microsoft in November update. This vulnerability allows victims to execute malicious code on victim machines No need to open infected files.
3. **Dynamic Data Exchange Protocol (DDE Exploit)** : an attacker uses built-in features on Microsoft Office called DDE to execute code on a victim's computer without turning on Macrio or interrupting memory.



Three vulnerabilities in MIcrosoft Office have been exploited to spread malware

Currently, these three vulnerabilities have been exploited to spread Zyklon malware via phishing emails, often in ZIP form and containing contaminated Office files.

When opened, this infected file runs a PowerShell script that will load the payload (Zyklon HTTP) on the victim's computer.*'These techniques share the domain to load the payload at the next level (Pause.ps1), which is another PowerShell script encoded with Base64'* , FireEye researchers said. *'Pause.ps1 handles the API needed to inject code. It also contains shellcode that can be injected. The injected code will load the payload from the server. The final payload is the PE executable file that is compiled with the .NET Framework '.*

Interestingly, the PowerShell script connects all IP addresses without dots (Dotless IP Address - eg http: 3627732942) to download the last payload.

* Dotless IP Address is sometimes called Decimal Address which is the decimal value of IPv4 address (indicated by dots between the numbers). Most browsers currently convert Decimal Address addresses to equivalent IPv4 addresses when opening with 'http:///'.

For example, Google's IP address 216.58.207.206 converted to decimal value will be http:/// 3627732942.

See more:

1. The unpatched Microsoft Word DDE vulnerability is exploited in a massive malware attack
2. 3 golden rules to avoid fake attacks
3. How to open the infected PowerPoint file, causing hackers to invade the computer?

According to BP