New malware uses Google Drive as a command-and-control server

Network security researchers have now discovered a new malware attack campaign linked to the notorious APH DarkHydrus group, which uses Google Drive as a command and control server.

In fact, most security tools will collect information related to network traffic to detect malicious IP addresses.Capturing this rule, attackers are increasingly applying more legal services infrastructure into their attacks to conceal malicious activities on cyberspace.

Network security researchers have now discovered a new malware attack campaign linked to the notorious APH DarkHydrus group, which uses Google Drive as a command and control server (command- and-control server - C2).

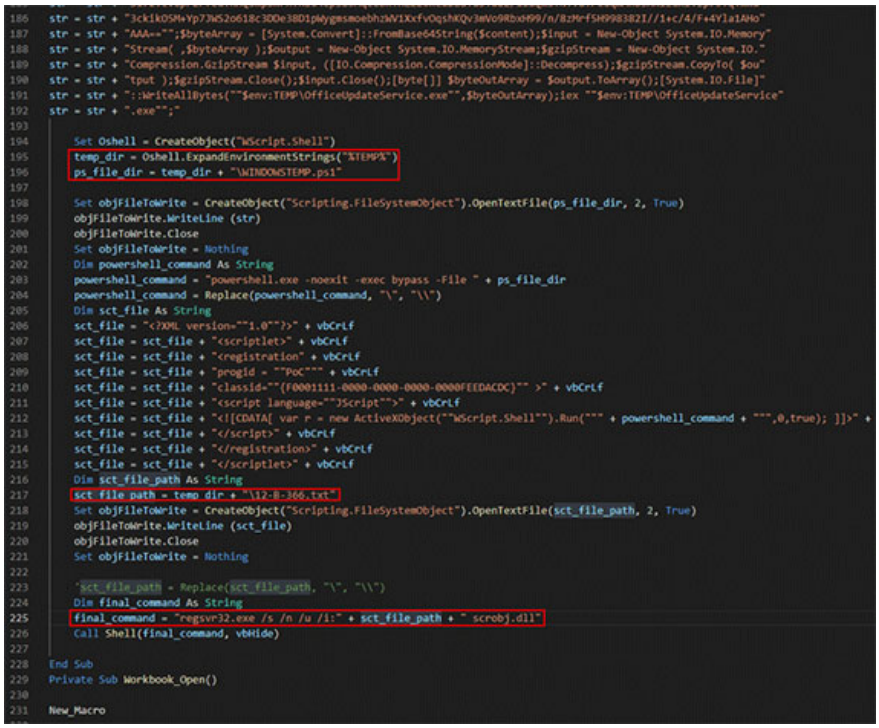
1. MySQL vulnerabilities allow malicious servers to steal data from customers

The DarkHydrus APT group first came to light in August last year when it was discovered that it is using open source Phishery tools to implement data collection campaigns against entities, agencies and organizations. government and education institutions in the Middle East.

According to a report published by 360 Security Intelligence Center (360TIC) and Palo Alto Networks, the latest malware attack campaign performed by the DarkTydrus APT team was also discovered to be an attack against goals in the Middle East.This time, attackers used a new Trojan variant they created, called RogueRobin.This malicious code is capable of infecting a victim's computer by tricking them into opening a Microsoft Excel

document containing the embedded VBA macro, instead of exploiting any Windows zero-day vulnerabilities as usual.

Enabling macros will remove a malicious text file (.txt) in the temporary directory and then make use of the legal 'personas.exe' application to run it, eventually installing the RogueRobin backlink written in the language. C # programming language on compromised systems.



According to Palo Alto researchers, RogueRobin comes with many stealth functions to avoid checking whether it is implemented in the sandbox environment, including checking the virtualization environment and memory. , the number of popular processors and analytics tools running on the system.In addition, it also contains anti-debug code.

Like the original version, the new variant of RogueRobin also uses DNS tunneling (DNS tunneling) - a technique for sending or retrieving data and commands through DNS query packets, to communicate with the command-and-server. -control its server.

1. Malware and user security bugs are found in top free VPN applications

However, the researchers also discovered that besides DNS tunneling, the malware was also designed to use the Google Drive API as an alternative channel to send data and receive commands from attackers.

"RogueRobin will upload a file to your Google Drive account and continuously check the file modification time to see if the victim has made any changes. The attacker will first modify the file to attach a code. The only identifier the Trojan will use to communicate in the future, 'Palo Alto experts say.

The new malware campaign shows that APT hacker groups are now moving more toward abuse of legitimate services for their command and control infrastructure to evade detection. of security tools.

Also note that because the VBA macro is a legitimate feature, most antivirus solutions will not flag any alerts or block any MS Office documents that come with the VBA code.

The best way to protect yourself from these new malware attacks is to never let your guard down against heavy documents, many of which are emailed, as well as not. ever allowed to click on any link within those documents, unless the source is verified.

See more:

1. Microsoft shook hands with VirusTotal in resolving malicious code issues that affected MSI files
2. 14 games on the App Store contain malicious code, iPhone users be careful
3. Windows Sandbox, a new feature in Windows 10 that helps create virtual machines for testing suspicious software
4. Warning: New extortion code GandCrab is attacking Vietnamese Internet users