Use SEO to bring Google search results to bank trojans

When you think you know all the tricks, malware teachers always have new tricks that surprise you.

When you think you know all the tricks, **malware** teachers always have new tricks that surprise you.

A group has released the **banking Zeus Panda trojans** since June this year. But instead of using traditional malicious spam and advertising techniques, the group has a new, unprecedented way of distributing **trojan banking** ever.

Black hat SEO?

Zeus Panda group used the network to hack the website, carefully insert a key into the new page or hide the key inside the existing page. They use Google SERP (Search Engine Results Page) to rank hacked pages at the top of the search results page for certain queries, related to banks and Personal Finance.

For example, when a person searches for 'Al Rajhi bank's working hours during Ramadan', the resulting infected links will appear on top of Google's search results page.

Taking advantage of Google's SERP to bring users to the infected page

Users who click on these links will be redirected to the hacked page, thereby executing malicious JavaScript code in the background and moving the user to a series of pages until downloading a Word file.

Combine spam SEO and malicious advertising

Date-redirected URL strings are used for malicious ad campaigns, taking users from maliciously advertised pages to phishing tools, phishing technical support or counterfeit software updates.

Basically, Zeus Panda incorporates SEO spam botnet (including hacked key pages to increase the SEO reputation of other sites) with a unique ad-redirect chain - familiar exploit tool.

The Word file that users download will be similar to what you get through spam emails. The difference is just how it gets into your computer.

New version of the bank Zeus Panda trojan

This Word file will be based on users turning on the executable macro, starting a script sequence to install a new variant of the Zeus Panda banking trojan, analyzed by G Data here.*https://cyber.wtf/2017/08/03/zeus-panda-down-to-the-roots/*

Cisco Talos - who discovered the Zeus Panda banking distribution campaign via malicious advertising with this SEO - also released a detailed report, including Google queries that infected pages will display and inform. Add more about the new variant of Zeus Panda.*http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html*

See also: 10 most effective antivirus software for Windows 2017