Issued 11/2/17

Group Uses SEO to Poison Google Search Results With Links to Banking Trojan

The Zeus Panda Group has taken a novel approach never before seen in the distribution of banking Trojans. This Zeus Panda group decided to rely on a network of hacked websites, on which they inserted carefully chosen keywords in new pages or hid the keywords inside existing pages.

The group leveraged the favorable Google SERP (Search Engine Results Pages) ranking of the hacked sites to position these malicious pages at the top of Google search results for specific queries related to online banking and personal finances. For example, a person searching for "al rajhi bank working hours in ramadan" would see a malicious link ranked at the top of Google search results. Users clicking on these links would arrive on the hacked site, from where malicious JavaScript code would execute in the background and redirected the user through a series of sites until he reached one offering a Word document for download. The Word document users got would be identical to the one someone would get if they received it via a spam email. The only difference would be how they got it, but not what was inside. The Word file still relies on users enabling macro execution, which starts a series of hidden scripts that install a new variant of the Zeus Panda banking Trojan.

This tangled chain of URL redirections is specific to malvertising campaigns that jolt users from sites running tainted ads to exploit kits, tech support scams, or fake software updaters.