Banking trojan Bolik spreads disguised as the NordVPN app

news.drweb.com/show/

Doctor Web

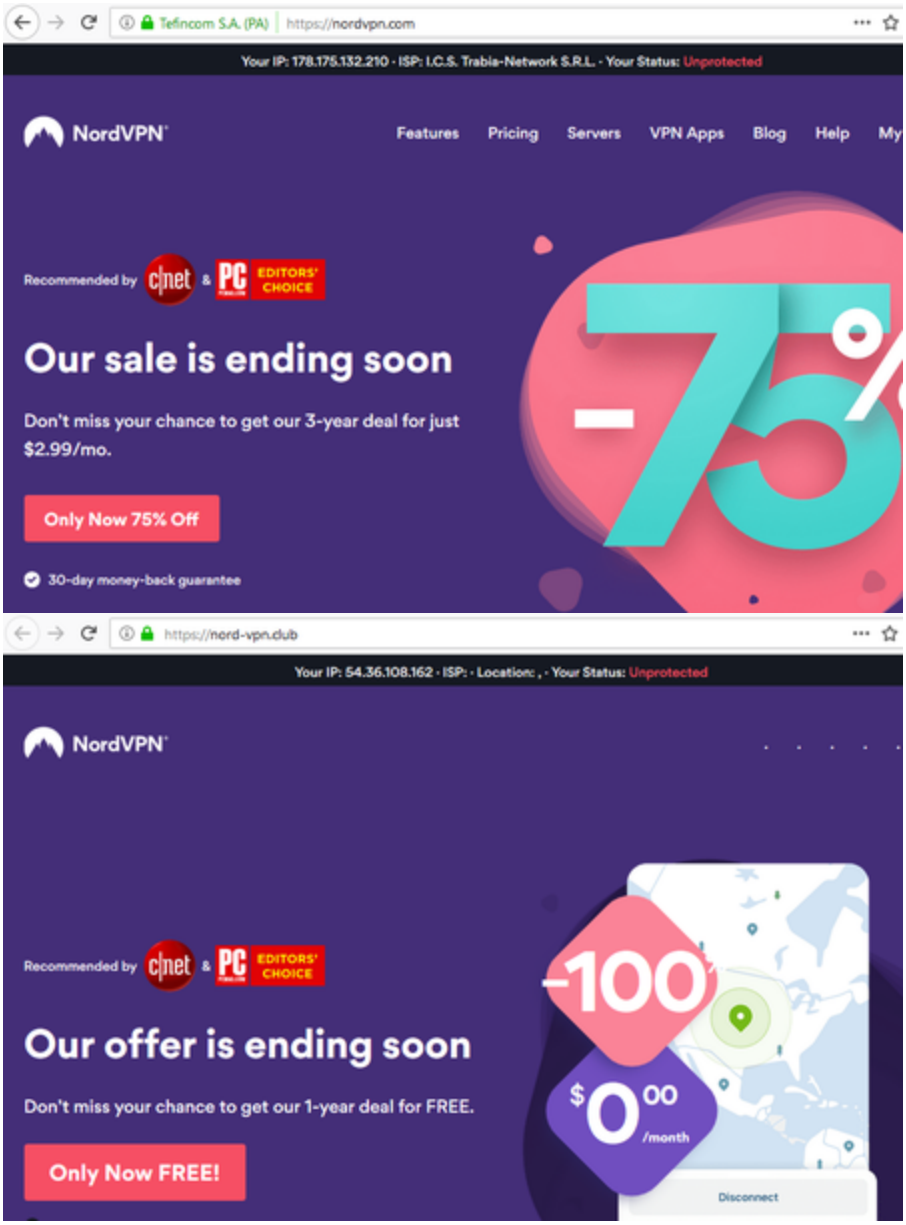
Back to news

August 19, 2019

Researchers at Doctor Web's virus lab discovered a dangerous banking trojan, Win32.Bolik.2, being spread by hackers via fake websites of popular software. One of these resources is copied from a well-known VPN service, while others are disguised as corporate office software sites.

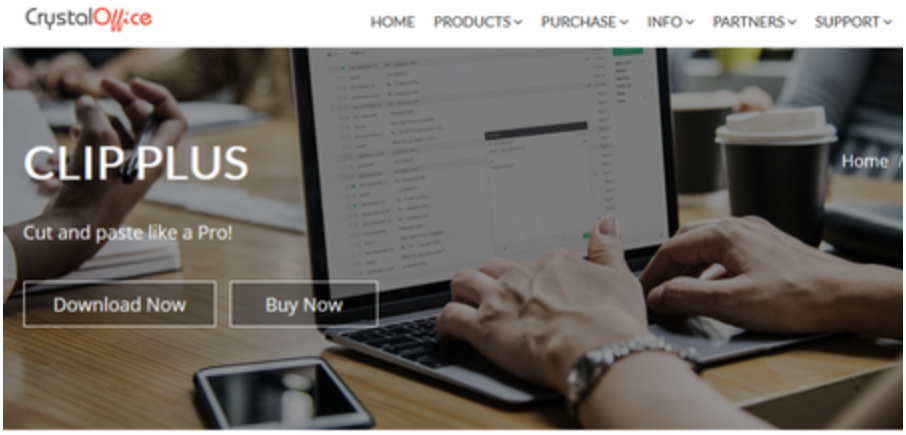
A copy of the NordVPN official website, which is a famous VPN service, was recently found by our researchers at nord-vpn[.]club. As with the original, it prompts users to download a program for using the VPN; but apart from the program itself, the fake authors distribute a dangerous banking trojan - **Win32.Bolik.2**.

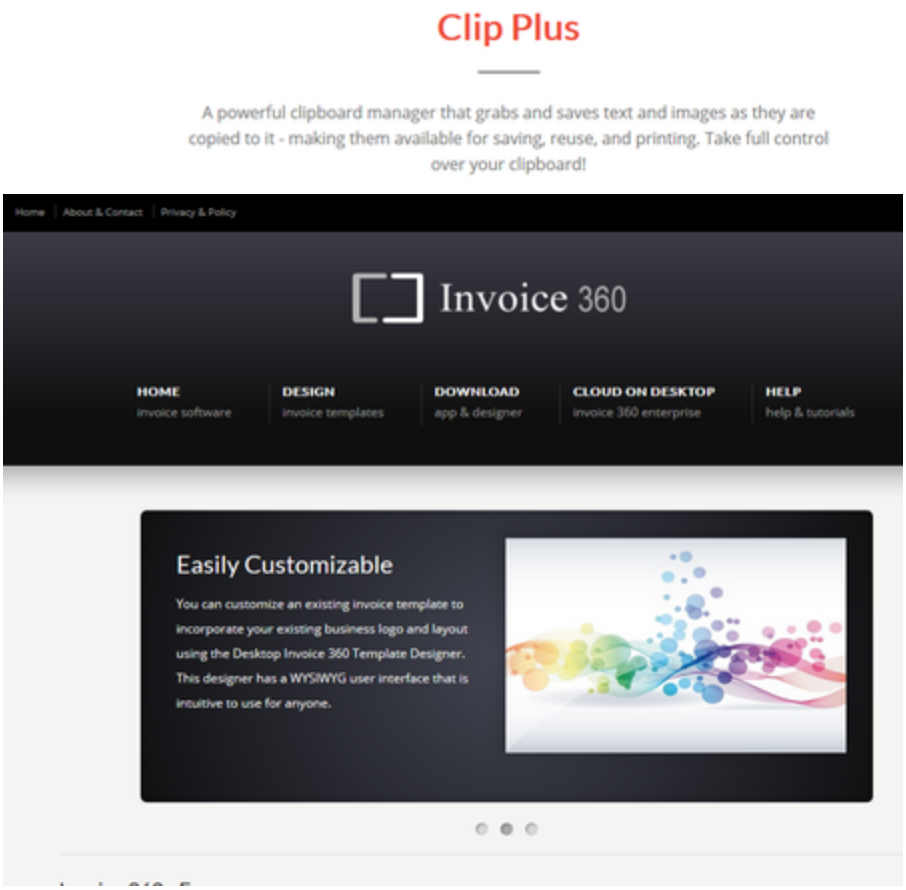
It has the same design, a similar domain name, and a valid SSL certificate.



According to our data, the malware campaign that uses those fake websites is primarily targeted at English-speaking audiences and was launched on August 8, 2019. However, at the time this news was released, the malicious fake NordVPN website already had thousands of visits.

On top of that, at the end of June this year, the same hacker group copied websites of office programs: invoicesoftware360[.]xyz (the original is invoicesoftware360[.]com) and clipoffice[.]xyz (the original is crystaloffice[.]com), where the **Win32.Bolik.2** trojan was distributed together with **Trojan.PWS.Stealer.26645** malware.





The **Win32.Bolik.2** trojan is an improved version of **Win32.Bolik.1** and has qualities of a multicomponent polymorphic file virus. Using this malware, hackers can perform web injections, traffic intercepts, keylogging and steal information from different bank-client systems.

Earlier this year, we reported another malware campaign from the same hacker group in which they distributed **Win32.Bolik.2** through a hacked video editing software website.

Both of these trojans are successfully detected and removed by Dr. Web products and pose no threat to our users.

Indicators of compromise

#banker #banking_trojan #stealer

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments