New AZORult campaign abuses popular VPN service to steal cryptocurrency

By Kaspersky

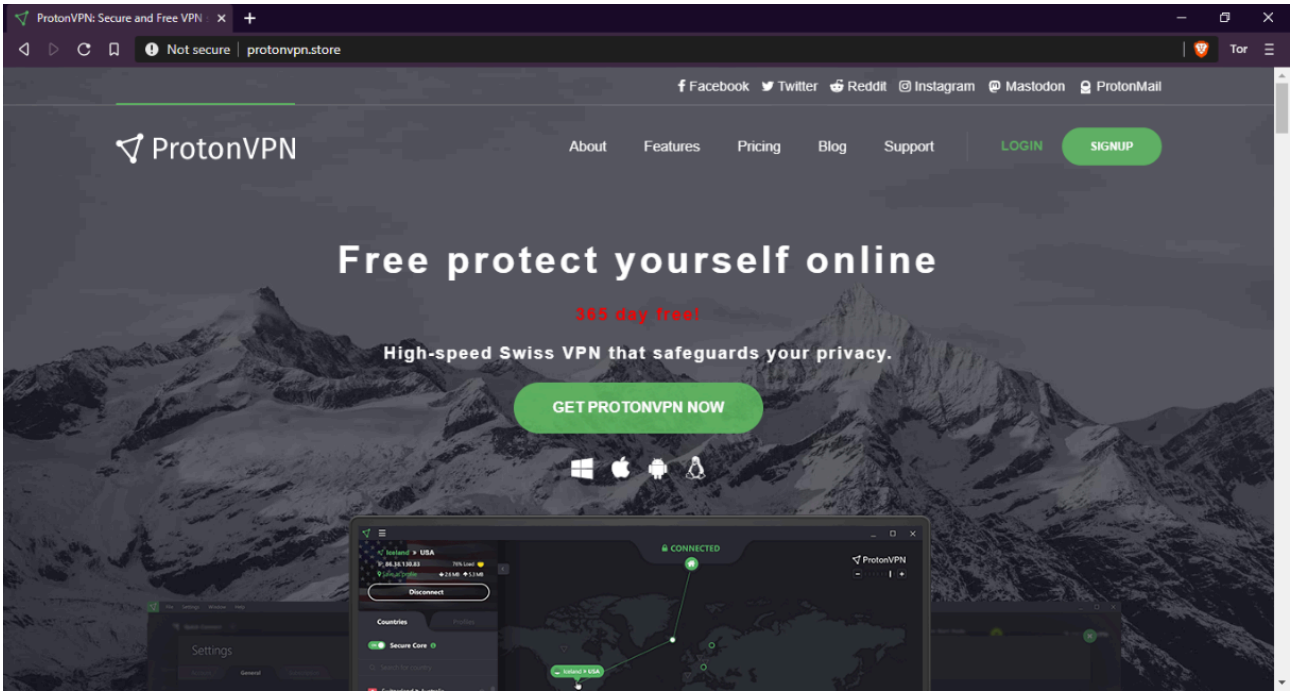
Published: 2020-02-18 · Archived: 2026-04-06 03:27:12 UTC

Kaspersky researchers have detected an unusual malicious campaign that uses a phishing copy of a popular VPN service's website to spread AZORult, a Trojan stealer, under the guise of installers for Windows.

The campaign, which kicked off at the end of November 2019 with the registration of a fake website, is currently active and focused on stealing personal information and cryptocurrency from infected users. This shows that cybercriminals are still hunting for cryptocurrency, despite reports that interest in the currency has died down.

AZORult is one of the most commonly bought and sold stealers on Russian forums due to its wide range of capabilities. This Trojan poses a serious threat to those whose computers may have been infected as it is capable of collecting various data, including browser history, login credentials, cookies, files from folders, cryptowallet files and can also be used as a loader to download other malware.

In a world where privacy is heavily fought for, VPN services play an important role by enabling additional data protection and safe internet browsing. Yet cybercriminals try to abuse the growing popularity of VPNs by impersonating them, as is the case in this AZORult campaign. In the most recent campaign, the attackers created a copy a VPN service's website, which looks exactly the same as the original with the only exception being a different domain name.



Screenshot of a phishing copy of the targeted VPN service's website

Links to the domain are spread through advertisements via different banner networks, a practice that is also called 'malvertizing'. The victim visits the phishing website and is prompted to download a free VPN installer. Once a victim downloads a fake VPN installer for Windows, it drops a copy of AZORult botnet implant. As soon as the implant is ran, it collects the infected device's environment information and reports it to the server. Finally, the attacker steals cryptocurrency from locally available wallets (Electrum, Bitcoin, Etherium, and others), FTP logins, and its passwords from FileZilla, email credentials, information from locally installed browsers (including cookies), credentials from WinSCP,Pidgin messenger and others.

Upon the discovery of the campaign, Kaspersky immediately informed the VPN service in question about the issue and blocked the fake website.

"This campaign is a good example of how vulnerable our personal data is nowadays. In order to protect it, users need to be cautious and be especially careful when surfing online. This case also shows why cybersecurity solutions are needed on every device. When it comes to phishing copies of websites, it is very difficult for the user to differentiate between a real and a fake version. Cybercriminals often capitalize on popular brands and this trend is not likely to die down", comments Dmitry Bestuzhev, head of GReAT in Latin America. "We strongly recommend using VPN for protection of data exchange on the web, but it is also important to closely study where the VPN software is downloaded from."

Kaspersky detects this threat as HEUR:Trojan-PSW.Win32.Azorult.gen

Read more about this AZORult campaign on Securelist.com.

To reduce the risk of infection with Trojan stealers such as AZORult, Kaspersky recommends users to:

- Check if the website is authentic. Do not visit websites until you are sure that they are legitimate and start with 'https'. Confirm that the website is genuine by double-checking the format of the URL or the spelling of the company name, reading reviews about it and checking the domain's registration data before starting downloads
- Store cryptocurrencies in cold wallets (ones that are not connected to the internet) to minimize risks of funds being stolen
- Try to keep your passwords and other personal information, including a wallet's private key, in a password manager - like Kaspersky Password Manager. The application securely stores your data in an encrypted private vault.
- Use a reliable security solution, such as Kaspersky Security Cloud, which protects devices from a wide range of threats, including phishing activity.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio

includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.
