AZORult spreads as a fake ProtonVPN installer

By Dmitry Bestuzhev

Published: 2020-02-18 · Archived: 2026-04-05 13:14:53 UTC

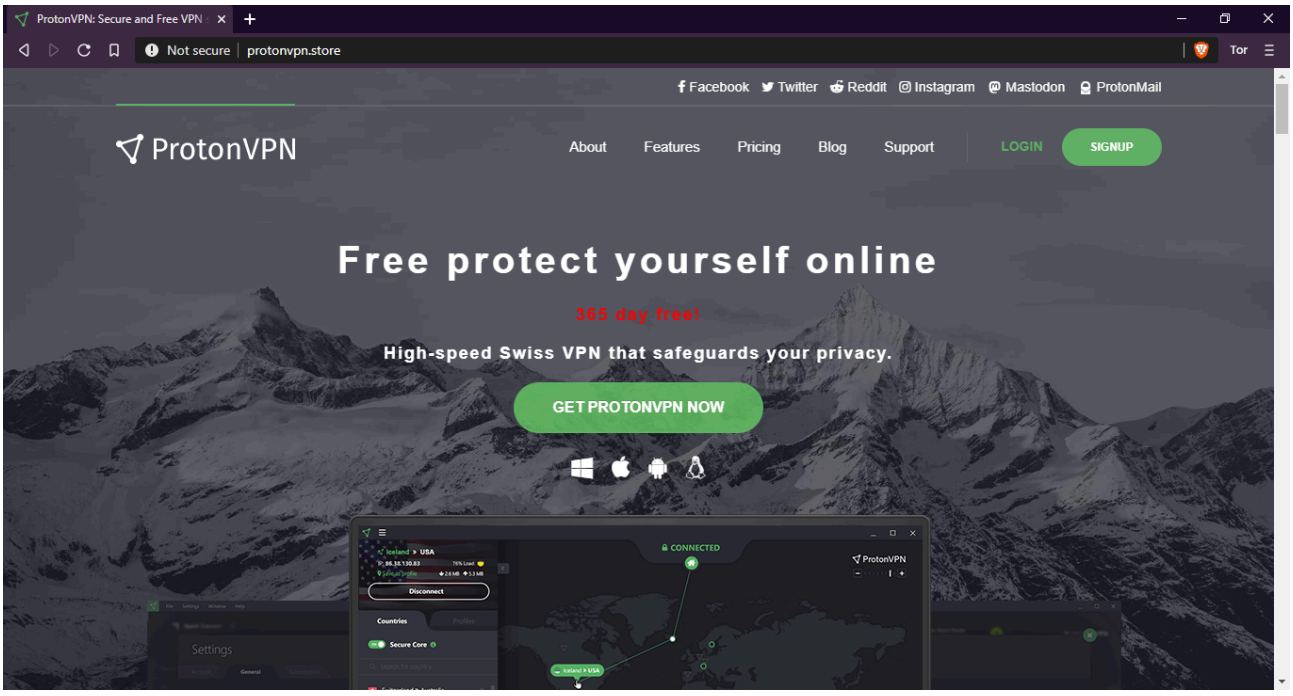
Incidents

Incidents

18 Feb 2020

1 minute read

AZORult has its history. However, a few days ago, we discovered what appears to be one of its most unusual campaigns: abusing the ProtonVPN service and dropping malware via fake ProtonVPN installers for Windows.

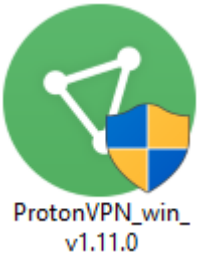


Screenshot of a fake ProtonVPN website

The campaign started at the end of November 2019 when the threat actor behind it registered a new domain under the name **protonvpn[.]store**. The Registrar used for this campaign is from Russia.

We have found that at least one of the infection vectors is through affiliation banners networks (Malvertising).

When the victim visits a counterfeit website and downloads a fake ProtonVPN installer for Windows, they receive a copy of the Azorult botnet implant.



The Website is an HTTrack copy of the original ProtonVPN website as shown below.

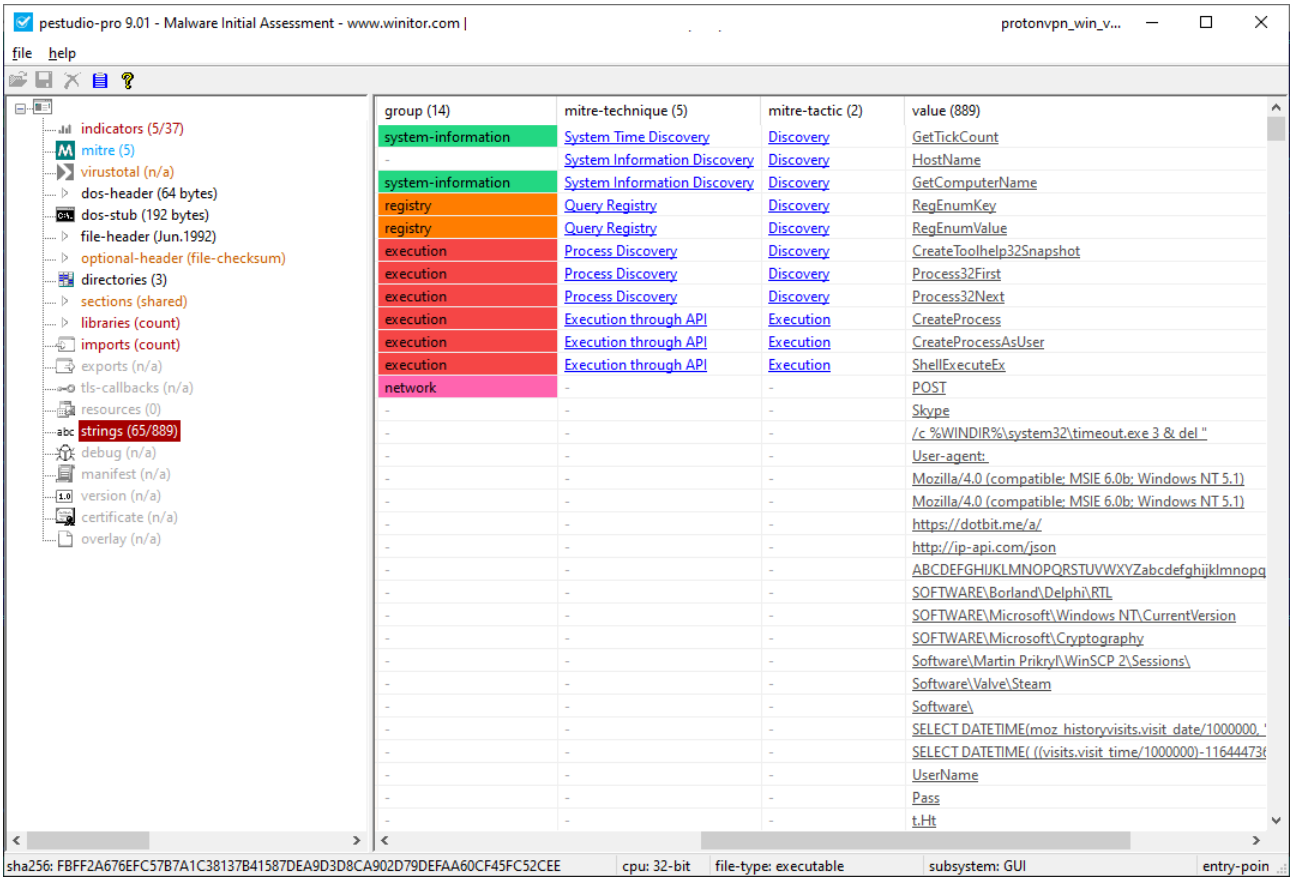
```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"></head><body><div
span> <span class="html-comment">&lt;!-- Added by HTTrack --&gt;</span><span class="html-tag">&lt
class="html-tag">&lt;head&gt;</span> <span class="html-tag">&lt;meta <span class="html-attribute-
attribute-value">Download the secure VPN client for ProtonVPN for free. Available as Windows VPN,
class="html-attribute-name">property</span>="<span class="html-attribute-value">og:url</span>" <s
also as Android VPN and iOS VPN client.</span>"&gt;</span> <span class="html-tag">&lt;meta <span
ProtonVPN</span>"&gt;</span> <span class="html-tag">&lt;meta <span class="html-attribute-name">na
name">name</span>="<span class="html-attribute-value">viewport</span>" <span class="html-attribut
```

Once the victim runs the implant, it collects the infected machine's environment information and reports it to the C2, located on the same **accounts[.]protonvpn[.]store** server.

```
{
 "config: ": [
  "MachineID :",
  "EXE_PATH  :",
  "Windows    :",
  "Computer(Username) :",
  "Screen:",
  "Layouts:",
  "LocalTime:",
  "Zone:",
  "[Soft]",
  "Host: User-Agent: Accept: ; charset=Content-Type:  HTTP/1.0POST text/*utf-8text/htmlHTTP/Proxy-AuthenticateAcceptContent-TypeContent-Lengthrealmhttp::Connection::connect: using proxy %1%http::Connection::connect: testing %1% for proxy routing"
 ]
```

```
}
```

In their greed, the threat actors have designed the malware to steal cryptocurrency from locally available wallets (Electrum, Bitcoin, Etherium, etc.), FTP logins and passwords from FileZilla, email credentials, information from locally installed browsers (including cookies), credentials for WinSCP, Pidgin messenger and others.



We have been able to identify a few samples associated with the campaign:

Filename	MD5 hash
ProtonVPN_win_v1.10.0.exe	cc2477cf4d596a88b349257cba3ef356
ProtonVPN_win_v1.11.0.exe	573ff02981a5c70ae6b2594b45aa7caa
ProtonVPN_win_v1.11.0.exe	c961a3e3bd646ed0732e867310333978
ProtonVPN_win_v1.11.0.exe	2a98e06c3310309c58fb149a8dc7392c
ProtonVPN_win_v1.11.0.exe	f21c21c2fceac5118ebf088653275b4f
ProtonVPN_win_v1.11.0.exe	0ae37532a7bbce03e7686eee49441c41
Unknown	974b6559a6b45067b465050e5002214b

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

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
