NordVPN
powered by NORD SECURITY

Online security starts with a click

Press Release

December 8, 2022
More information: darija@nordsec.com

Data of 600 thousand Indians for sale on bot markets

This growing threat has already affected five million people globally, with hackers selling webcam snaps, screenshots, up-to-date logins, cookies, and digital fingerprints

At least **five million** people have had their online identities stolen and sold on bot markets for **490 INR** on average. Out of all the affected people, 600 thousand are from India, making the country the most affected by this threat in the world.

This data comes from research by the cybersecurity company NordVPN, which looked into three major bot markets. The word "bot" in this situation does not mean an autonomous program – in this case, it refers to data-harvesting malware. Bot markets are online marketplaces hackers use to sell data they have stolen l from their victims' devices with bot malware. The data is sold in packets, which include logins, cookies, digital fingerprints, and other information — the full digital identity of a compromised person.

"What makes bot markets different from other dark web markets is that they are able to get large amounts of data about one person in one place. And after the bot is sold, they guarantee the buyer that the victim's information will be updated as long as their device is infected by the bot," says Marijus Briedis, CTO at NordVPN. "A simple password is no longer worth money to criminals, when they can buy logins, cookies, and digital fingerprints in one click for just 490 rupees."

Researchers analyzed three major bot markets: the Genesis Market, the Russian Market, and 2Easy. All of the markets were active and accessible on the surface web at the time of analysis. The data on bot markets was compiled in partnership with independent third-party researchers specializing in cybersecurity incident research.

The most popular types of malware that steal data are RedLine, Vidar, Racoon, Taurus, and AZORult.

What information do hackers sell on bot markets?

- **Screenshots of a device.** During a malicious attack, a virus might take a snapshot of the user's screen. It can even take a picture with the user's webcam.

- **Logins and other credentials.** When a virus attacks the user's device, it may grab logins saved to their browser. The research found **26.6 million** stolen logins on the analyzed markets. Among them were 720 thousand Google logins, 654 thousand Microsoft logins, and 647 thousand Facebook logins.[1]

- **Cookies.** These are also usually stolen from a user's browser and help criminals bypass two-factor authentication. The research found **667 million** stolen cookies on the analyzed markets.

- **Digital fingerprints.** A person's digital fingerprint includes screen resolution, device information, default language, browser preferences, and other information that makes the user unique. Many online platforms track their users' digital fingerprints to make sure they properly authenticate them. During the research, **81 thousand** stolen digital fingerprints were found on the analyzed markets.

- **Autofill forms.** Many people use the autofill function for their names and emails as well as for their payment cards and addresses. All of these details can be stolen by malware. During the research, **538 thousand** autofill forms were found on the analyzed market.

You can learn more about how bot markets work by watching this video: https://youtu.be/dAyl1xBgTUg

A perfect crime using bots

The scariest thing about bot markets is that they make it easy for hackers to exploit the victim's data. Even a rookie cybercriminal can connect to someone's Facebook account if they have cookies and digital fingerprints in place, which help them bypass multi-factor authentication.

After logging in to a user's account, a cybercriminal can try contacting people on a victim's friends list and send malicious links or ask for a money transfer. They can also post fake information on the victim's social media feed.

Information stolen from autofill forms or just by taking a device screenshot can help these actions look more believable and trustworthy. And you will have no way to detect who used your data.

"Some tactics are even simpler. A hacker can, for example, take control of a victim's Steam account by changing the password. Steam accounts are sold for up to $6,000 per account and can be easy money for a criminal," says Marijus Briedis.

[1] The rest of the stolen logins are indicated in the table "Stolen logins found on bot markets" below.

More sophisticated criminals buy this information and target businesses with phishing attacks, trying to impersonate the company's employees.

"To protect yourself, use an antivirus at all times. Other measures that could help – a password manager and file encryptions tools to make sure that even if a criminal infects your device, there is very little for them to steal," adds Marijus Briedis.

The methodology, together with more information about the three analyzed markets, can be found here: https://nordvpn.com/research-lab/bot-markets/

The price of a bot was converted to local currency (from US dollars to INR) on November 29th.
Data about the number of internet users in certain countries was taken from DataReportal.

ABOUT NORDVPN

NordVPN is the world's most advanced VPN service provider, used by millions of internet users worldwide. NordVPN provides double VPN encryption and Onion Over VPN, guaranteeing privacy with zero tracking. One of the key features of the product is Threat Protection, which blocks malicious websites, malware, trackers, and ads. NordVPN is very user friendly, offers one of the best prices on the market, and has over 5,000 servers in 60 countries worldwide. For more information: nordvpn.com

Stolen logins found on bot markets

Google	720,676
Microsoft	654,444
Facebook	647,574
Amazon	226,264
Netflix	223,173
PayPal	201,649
Instagram	196,904
Steam	180,581
Ebay	123,955
EA Network	115,807
Roblox	112,050
LinkedIn	108,789
Yahoo	105,944
Dropbox	105,918
Ali Express	100,690
Twitch	93,678
Apple Store	90,068

Twitter	89,469
Sony Entertainment	89,421
Spotify	75,941
Riot Games	75,242
Epic Games	72,673
MEGAnz	61,150

IMAGE