Data Breach TODAY
Prevention. Response. Notification.
https://www.databreachtoday.com/

Account Takeover , Cybercrime , Fraud Management & Cybercrime

5 Billion Unique Credentials Circulating on Darknet

Bank Account Credentials Sell for an Average of $71, Report Finds

Ishita Chigilli Palli (Ishita_CP) • July 10, 2020

Banking and financial credentials are the most common listings on darknet sites (Source: Digital Shadows)

Five billion unique user credentials are circulating on darknet forums, with cybercriminals offering to sell access to bank accounts as well as domain administrator access to corporate networks, according to the Photon Research Team at security firm Digital Shadows.

See Also: Live Webinar | Why APTs Can Be So Difficult To Find, Investigate, And Resolve

Researchers found that more than 15 billion user credentials are in circulation, of which 5 billion username and password combinations don't have repeated credential pairs and have been advertised on underground forums only once, according to the report released this week.

"More often than not, credentials that are exposed are reposts or amalgamations of previously exposed credentials," says Kacey Clark, a threat researcher at Digital Shadows. "Security teams that monitor for these types of issues, therefore, may well have already remediated the risk. Unique credentials, however, represent a higher risk and so are likely of greater concern for security teams."

There's been a 300% increase in the number of stolen credentials circulating on these underground forums since 2018. After an 18-month research effort, the researchers estimate that the credentials stem from nearly 100,000 data breaches that have taken place over the last two years, according to Digital Shadows (see:

Stolen Zoom Credentials: Hackers Sell Cheap Access).

"I'm not overly surprised by the numbers," Troy Hunt, creator of the HaveIBeenPwned breach notification service, tells Information Security Media Group. "Anecdotally, I've noticed a lot more credential stuffing lists in circulation recently, and just like the [COVID-19] pandemic itself, they seem to be replicating at a fierce rate."

High-End Accounts

Cybercriminals employ a variety of techniques to carry out account takeovers. Some criminals buy credentials on darknet marketplaces, where a single account costs on average $15.43. But the more sought-after banking credentials sell for an average of $71, according to the report.

The price for access to a single bank account can exceed $500 depending on factors such as the amount of money in the account, the availability to access personally identifiable information and the account's age, the report notes.

The advertisements for access to these types of high-end accounts comprised 25% of all advertisements on underground sites analyzed by Digital Shadows.

In addition, the researchers found that credentials for domain administrator access to corporations and government agencies, where there is potential for a complete network compromise, can be sold for as high as $140,000 if a bidding war takes place. But the average selling price is about $3,100, according to the report.

To give a potential buyer of admin credentials additional information to help make a sale, some underground forums include details such as the number of devices running on the network, how many employees work at the company and any intellectual property or sensitive documents on the system, the report states.

"Cybercriminals target the obvious goldmines of financial or internal company accounts, but they also see value in things like streaming or anti-virus accounts," Clark tells ISMG.

For example, video game account credentials sell for as little as $2, the report notes.

Many individuals use the same credentials across multiple platforms, researchers at Digital Shadows note. This leaves users vulnerable to account takeovers by hackers implementing brute-force attacks. And the tools for such attacks can be purchased on the darknet for an average price of $4, according to the report.

Harvesting Credentials

Apart from buying credentials directly on the darknet, cybercriminals also use brute-force cracking tools and account checkers to steal information, according to the report. "Based on their descriptions, these tools can 'crack' accounts associated with banking, video games, e-commerce services, social media, streaming, VPN accounts and proxy services," the report notes.

Many hackers also harvest banking credentials using Trojans, keyloggers and man-in-the-middle browser attacks, which enable them to steal the data directly from victims' online banking portals, according to the report.

Once a hacker obtains a list of credentials, they can then buy or rent tools for credential-stuffing attacks - automated login attempts using a combination of usernames and plaintext passwords, the report notes.

The Digital Shadows researchers also note that some sites rent out identity credentials for a limited amount of time for less than $10. These sites offer not just access to compromised accounts, but also browser data, such as IP addresses, time zones and cookies, which make it easier to avoid detection, according to the report.

Cybercriminals also sometimes share credentials for free on forums to help build a sense of community, Clark says. "After someone posts a hashed data set, other forum users work on dehashing it and then post the plaintext passwords as a database."

Managing Editor Scott Ferguson contributed to this report.

About the Author

Ishita Chigilli Palli

Senior Correspondent, Global News Desk

As senior correspondent for Information Security Media Group's global news desk, Ishita covers news worldwide. She previously worked at Thomson Reuters, where she specialized in reporting breaking news stories on a variety of topics.