



Hackers Stole Nearly 26 Million User Login Credentials for Sites Like Amazon, Google, Facebook

Description

Hackers using a custom Trojan-type malware stole nearly 26 million login credentials – emails or usernames and associated passwords – from almost a million websites over a two year period, including from such namesakes as Amazon, Facebook, and Twitter, according to cybersecurity provider [NordLocker](#).



A hacker in China on Aug. 4, 2020. (Nicolas Asfour/AFP via Getty Images)

The malware infiltrated over 3 million Windows-based computers between 2018 and 2020, with the cyber intruders making off with around 1.2 terabytes of personal information, according to a case study carried out by NordLocker in partnership with a third-party firm specializing in data breach analysis.

The 26 million stolen login credentials were across twelve different website types, including social media, online gaming, and email services. **They included such household names as Google (1.54 million), Facebook (1.47 million), Amazon (0.21 million), Apple (0.13 million), Netflix (0.17 million), and PayPal (0.15 million).**



An illustration file photograph shows the logos of Google, Apple, Facebook, Amazon, and Microsoft displayed on a mobile phone and a laptop screen. (Justin Tallis/AFP via Getty Images)

In addition to login credentials, the stolen data includes 1.1 million unique email addresses, over 2 billion cookies, and 6.6 million files that users were storing on their desktops and in their downloads folders.

The stolen cookies, which can in some cases give access to a victim's online accounts, were sorted into five groups: online marketplace, online gaming, file sharing site, social media, and video streaming services.

The billions of stolen cookies were associated with such sites as YouTube (17.1 million), Facebook (8.1 million), Twitter (5.2 million), Amazon (3.5 million), MediaFire (3.2 million), and eBay (2 million).

The malware mainly targeted web browsers to steal the data, with the top three software sources for stolen email/usernames plus passwords being Google Chrome (19.4 million), Mozilla FireFox (3.3 million), and Opera (2 million).

Besides stealing files, the malware also took screenshots of infected computers and photos using its webcam.

The malware was transmitted by email and pirated software, including illegal versions of Adobe

Photoshop 2018 and a number of cracked games.

The report comes amid warnings from administration officials that cyberattacks of various types are on the rise.

U.S. Secretary of Commerce Gina Raimondo said last week that the number of cyber intrusions will only increase in the future, and urged businesses to shore up their cybersecurity systems.

“We should assume and businesses should assume that these attacks are here to stay and if anything will intensify,” Raimondo said in an [interview with ABC](#).

Her remarks followed a June 3 letter from Anne Neuberger, a cybersecurity adviser at the National Security Council, who warned business leaders about the growing risk of ransomware attacks and urged them to beef up security measures.

“The threats are serious and they are increasing,” [Neuberger said](#) in the letter obtained by media outlets.

The officials’ warnings come after a number of recent high-profile cyberattacks, including one targeting Colonial Pipeline last month, leading to a disruptive shutdown and gasoline shortages, and another targeting JBS, America’s biggest beef producer.

by Tom Ozimek

Date Created

June 2021