FBI warns of hackers selling credentials for U.S. college networks

By
Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)

May 27, 2022 04:26 PM **0**

Cybercriminals are offering to sell for thousands of U.S. dollars network access credentials for higher education institutions based in the United States.

This type of advertisement is present on both publicly available cybercriminal online forums as well as marketplaces on the dark web.

Thousands of creds for sale

The Federal Bureau of Investigation (FBI) has issued an alert about usernames and passwords giving access to colleges and universities based in the U.S. are available for sale on Russian cybercriminal forums.

(https://www.bleepingcomputer.com/news/security/github-attackers-stole-login-details-of-100k-npm-user-accounts/?traffic_source=Connatix)

GitHub: Attackers stole login details of 100K npm user accounts

The sensitive information consists of network credentials and virtual private network (VPN) access "to a multitude" of higher education organizations in the U.S.

In some cases, the seller posted a screenshot proving that the credentials provide the advertised access.

The price for such credentials varies between a few U.S. dollars to thousands, the agency says in an alert released this week.

Cybercriminals have several methods to collect usernames and passwords, phishing being among the most common. Testing credentials from emails associated with a higher education organization, obtained from breaches at various online services, is also a frequent practice.

> "Credential harvesting against an organization is often a byproduct of spear-phishing, ransomware, or other cyber intrusion tactics" - the Federal Bureau of Investigation (https://www.ic3.gov/Media/News/2022/220526.pdf)

Network access is often used by ransomware gangs to gain access to a victim and engage in lateral movement activity to compromise valuable hosts and encrypt them for a ransom payment.

Credentials are many times advertised by actors specialized in stealing sensitive information and sold for prices that depend on the victim and the type of access.

The FBI notes that in May last year a group likely involved in trafficking login credentials posted more than 36,000 email and password combinations, an indication.

Security recommendations

The agency recommends academic entities adopt mitigation strategies that reduce the risk of compromise. Applying updates as they become available and checking for end-of-life notifications are at the top of the list.

Implementing brute-force protection, training sessions for students and faculty to identify phishing attempts, using strong, unique passwords, and multi-factor authentication are regular recommendations that are valid for all organizations.

The FBI also advises reducing credential exposure by restricting where accounts can be used and enabling local device credential protection mechanisms.

Network segmentation along with monitoring for abnormal traffic can prevent malware from spreading and detect anomalies indicative of malicious activity.

Special attention should be given to connections via the remote desktop protocol (RDP), which is a frequent target for hackers.