Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

26 May 2022

PIN Number

20220526-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums

Summary

The FBI is informing academic partners of identified US college and university credentials advertised for sale on online criminal marketplaces and publically accessible forums. This exposure of sensitive credential and network access information, especially privileged user accounts, could lead to subsequent cyber attacks against individual users or affiliated organizations.

Threat

Cyber actors continue to conduct attacks against US colleges and universities leading to the exposure of user information on public and cyber criminal forums. Credential harvesting against an organization is often a byproduct of spear-phishing, ransomware, or other cyber intrusion tactics. For example, in 2017, cyber criminals targeted universities to hack *.edu* accounts by cloning university login pages and embedding a credential harvester link in phishing emails. Successfully harvested credentials were then sent to the cyber criminals in an automated email

from their servers. Such tactics have continued to prevail and ramped up with COVID-themed phishing attacks to steal university login credentials, according to security researchers from a US-based company in December 2021.

The FBI has observed incidents of stolen higher education credential information posted on publically accessible online forums or listed for sale on criminal marketplaces. The exposure of usernames and passwords can lead to brute force credential stuffing computer network attacks, whereby attackers attempt logins across various internet sites or exploit them for subsequent cyber attacks as criminal actors take advantage of users recycling the same credentials across multiple accounts, internet sites, and services. If attackers are successful in compromising a victim account, they may attempt to drain the account of stored value, leverage or re-sell credit card numbers and other personally identifiable information, submit fraudulent transactions, exploit for other criminal activity against the account holder, or use for subsequent attacks against affiliated organizations.

- As of January 2022, Russian cyber criminal forums offered for sale or posted for public access the network credentials and virtual private network accesses to a multitude of identified US-based universities and colleges across the country, some of which included screenshots as proof of access. Sites posting credentials for sale typically listed prices varying from a few to multiple thousands of US dollars.

- In May 2021, over 36,000 email and password combinations (some of which may have been duplicates) for email accounts ending in *.edu* were identified on a publically available instant messaging platform. The group posting the compromised data appeared to be involved in the trafficking of stolen login credentials and other cyber criminal activities.

- In late 2020, US territory-based university account usernames and passwords with the domain *.edu* were found for sale on the dark web. The seller listed approximately 2,000 unique usernames with accompanying passwords and asked for donations be made to an identified bitcoin wallet. As of early 2022, the site containing the credentials was no longer accessible.

Recommendations

The FBI recommends colleges, universities, and all academic entities establish and maintain strong liaison relationships with the FBI Field Office in their region. The location and contact information for all FBI Field Offices can be located at www.fbi.gov/contact-us/field-offices. Through these partnerships, the FBI can assist with identifying vulnerabilities to academia and mitigating potential threat activity.

The FBI further recommends that academic entities review and, if needed, update incident response and communication plans that list actions an organization will take if impacted by a

cyber incident. In addition, consider the following mitigation strategies to reduce the risk of compromise:

- Keep all operating systems and software up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Regularly check for software updates and end of life (EOL) notifications, and prioritize patching known exploited vulnerabilities. Automate software security scanning and testing when possible.
- Implement user training programs and phishing exercises for students and faculty to raise awareness about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments.
- Require strong, unique passwords for all accounts with password logins and establish lock-out rules for incorrect password attempts. Avoid password reuse across multiple accounts or stored on the system where an adversary may gain access.
- Require multi-factor authentication (MFA), preferably using phishing-resistant authenticators, for as many services as possible - particularly for accounts that access critical systems, webmail, virtual private networks (VPN), and privileged accounts that manage backups.
- Reduce credential exposure and enforce credential protection by restricting where accounts and credentials can be used and by using local device credential protection features.
- Segment networks to help prevent unauthorized access by malicious actors or the spread of malware.
- Identify, detect, and investigate abnormal activity with network-monitoring tools that log and report all network traffic, including lateral movement on a network.
- Use anomaly detection tools that identify an unusual increase in traffic and failed authentication attempts.
- Enforce principle of least privilege through authorization policies. Account privileges should be clearly defined, narrowly scoped, and regularly audited against usage patterns.
- Secure and closely monitor remote desktop protocol (RDP) use.
    - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. If RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.
    - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).

  - Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
  - Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
  - Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
- Document external remote connections. Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.