Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

7 February 2019

PIN Number
20190207-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

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 criminals.

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Criminals Conducting Successful Spearphishing Campaigns Against Students at Multiple Universities

Summary

The FBI has identified successful spearphishing campaigns directed at college and university students, especially during periods when financial aid funds are disbursed in large volumes. In general, the spearphishing emails request students' login credentials for the University's internal intranet. The cyber criminals then capture students' login credentials, and after gaining access, change the students' direct deposit destination to bank accounts within the threat actor's control.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat

In February 2018, the FBI received notification of a spearphishing campaign targeting students at an identified University in the south eastern United States. The campaign occurred in January 2018 when an unidentified number of students attending the University received an email requesting their login credentials for the University's internal intranet. Using the University's intranet portal, the cyber criminals accessed a third-party vendor that manages the disbursement of financial aid to students and changed the direct deposit information for 21 identified students to bank accounts under the cyber criminal's control. The threat actor stole approximately $75,000 from the 21 students. The student accounts were accessed by at least 13 identified US Internet Protocol (IP) addresses.

On 31 August 2018, the Department of Education identified a similar spearphishing campaign targeting multiple institutions of higher education. In this campaign, the cyber criminals sent students an email inviting them to view and confirm their updated billing statement by logging into the school's student portal. After gaining access, the cyber criminals changed the students' direct deposit destinations to bank accounts under the threat actor's control.

The nature of the spearphishing emails indicates the cyber criminals conducted reconnaissance of the target institutions and understand the schools' use of student portals and third-party vendors for processing student loan payment information. In addition, the timing of the campaigns indicates the cyber criminals almost certainly launched these campaigns to coincide with periods when financial aid funds are disseminated in large volumes.

Recommendations

The FBI recommends providers implement the preventative measures listed below to help secure their systems from attacks:

- Notify all students of the phishing attempts and encourage them to be extra vigilant
- Implement two-factor authentication for access to sensitive systems and information
- Monitor student login attempts from unusual IP addresses and other anomalous activity
- Educate students on appropriate preventative and reactive actions to known criminal schemes and social engineering threats

- Apply extra scrutiny to e-mail messages with links or attachments directed toward students
- Apply extra scrutiny to bank information initiated by the students seeking to update or change direct deposit credentials
- Direct students to forward any suspicious requests for personal information to the information technology or security department

For recent guidance on mitigation strategies against spearphishing and network infrastructure targeting, please refer to the following joint technical alerts:

- https://www.us-cert.gov/ncas/alerts/TA18-074A
- https://www.us-cert.gov/ncas/alerts/TA18-106A

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by email at CyWatch@fbi.gov. 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: GREEN**. Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey