Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

31 January 2018

PIN Number

20180131-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force**, **FBI CyWatch, or the U.S. Department of Education's Office of Inspector General Technology Crimes Division (ED OIG/TCD)**

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

E-mail:
cywatch@fbi.gov
TCD.IR@ed.gov

Phone:
1-855-292-3937 (FBI)
202-245-6550 (ED OIG/TCD)

The following information is being provided by the FBI and the Department of Education's Office of the Inspector General, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP:AMBER**: Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Cyber Criminal Group Threatens Schools and Students

This notification was created jointly by the FBI with the U.S. Department of Education's Office of the Inspector General.

Summary

Since April 2016, a loosely affiliated group of highly trained hackers calling themselves TheDarkOverlord (TDO) have conducted various extortion schemes with a recent focus on the public school system. TDO used remote access tools to breach school district networks and then proceeded to steal sensitive data. To extort money from its victims, including students, TDO threatened violence or the release of stolen sensitive data.

Threat

As of January 2018, TDO was responsible for at least 69 intrusions into schools and other businesses, the attempted sale of over 100 million records containing personally identifiable information (PII), and the release of over 200,000 records including the PII of over 7,000 students due to nonpayment of ransoms.

TDO typically opens communications via e-mail with veiled threats of publicly releasing or selling the victim's sensitive information. However, in September 2017, TDO escalated its tactics by threatening school shootings through text messages and emails directed at students, staff, and local law enforcement officials. As a result, several schools receiving these threats shut down for one or more days as a safety precaution. TDO then contacted the school districts several days later, demanding payment to prevent the release of student data on the internet.

TDO engages in a pattern of verbal abuse and threats of violence during communication with victims, regardless of the victims' willingness to pay extortion demands. In a recent incident, TDO threatened to publicize the sensitive behavioral reports and private health information of students. Throughout September and October 2017, TDO was reportedly connected to multiple threats of violence on school campuses, often prior to extortion attempts. These threats caused panic, but provided TDO with no apparent monetary gain.

Recommendation

The FBI does not support paying a ransom to criminals. Paying a ransom does not guarantee an organization will regain access to their data. Paying a ransom emboldens the criminal to target other organizations for profit and provides a lucrative environment for other criminals to become involved. Finally, by paying a ransom, victims are funding illicit activity associated with criminal groups, and potentially terrorist groups, who will continue to target organizations for profit. While the FBI does not support paying a ransom, it is understood executives will evaluate all options to protect their organizations and those they serve. If you have received an extortion demand:

- Contact law enforcement immediately
- Retain the original emails with headers
- If applicable, maintain a timeline of the attack, recording all times and content of the attack.

IT best practices to protect against network intrusions:

- Change passwords and do not reuse passwords for multiple accounts
- If possible, use two factor authentication
- Be careful when providing contact information
- Beware of social engineering tactics aimed at revealing sensitive information
- Audit which accounts are utilizing remote access
- Establish whitelist access for any remote access
- Consider disabling remote access if not in use

- Audit logs for all remote connection protocols
- Audit all user accounts with admin privileges to ensure they are authorized for that role
- Audit logs to ensure all new accounts were intentionally created
- Scan for open or listening ports and remediate
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location
- Backup copies of sensitive data should not be readily accessible from local networks
- Ensure software or firmware updates are applied as soon as the device manufacturer releases them

Administrative Note

This product is marked **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

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