Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 June 2020

PIN Number
20200623-001

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 actors. This product was coordinated with DHS-CISA.

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

Ransomware Targeting of K-12 Schools Likely to Increase During the COVID-19 Pandemic

Summary

The FBI is providing situational awareness to stakeholders in the K-12 educational system during the COVID-19 pandemic regarding the ransomware threat. Cyber actors are likely to increase targeting of K-12 schools during the COVID-19 pandemic because they represent an opportunistic target as more of these institutions transition to distance learning. K-12 schools have increased their reliance on technology for different school operations, such as teaching, learning, or administrative functions. This shift has created greater risks for schools, as they now must depend on remote tools. In general, however, K-12 institutions have limited resources to dedicate to network defense, leaving them vulnerable to cyber attacks. Furthermore, public pressure and the threat of releasing victim data may create an elevated urgency for schools to pay ransoms.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Cybersecurity industry reporting indicates that ransomware continues to rise among K-12 schools and represents the second most targeted group of victims behind municipalities. According to an antivirus company, in 2019, 1,233 individual schools were potentially affected by ransomware attacks, while in the first quarter of 2020 there were already approximately 422 individual schools affected.

Threat

- Since at least September 2019, the FBI has observed an increase in ransomware attacks targeting K-12 schools through remote desktop protocol (RDP) vulnerabilities, particularly the Ryuk[a] variant.
- The aforementioned ransomware attacks against K-12 schools have occurred with varying levels of debilitating damage, from affecting various systems[b] to complete shutdown.
- According to an educational network security firm, cyber actors using ransomware have shifted to threatening to release victim data publicly, in addition to leaving systems locked if ransom demands are not met.

Recommendations

The FBI does not encourage paying a ransom to cyber actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that when schools are faced with an inability to function, administrators will evaluate all options to protect their communities. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks. In addition to the above recommendations, the following actions are also suggested:

[a] Ryuk – A form of ransomware that blocks access to a system or device using encryption. Ryuk is generally deployed via email phishing or exploitation of RDP.

[b] K-12 school systems can encompass, but is not limited to, those that provide administrative, financial, management, and communication capabilities.

- Retain multiple uninfected backups of critical data and applications. These backups should be air-gapped and password protected.
- Develop an approved white list of applications and processes allowed to run in your environment.
- Use File Integrity Monitoring to detect changes of critical OS files and processes.
- Follow the principle of Least Privilege for Access Control. Each user should have the least privileges needed for their job.
- Have penetration testing conducted by experts to ensure your organization is maintaining an acceptable security posture.
- Monitor or block IP addresses from known malicious actors.
- Educate your workforce on current and emerging cybersecurity risks and vulnerabilities.
- Implement endpoint protection solutions such as antivirus and antimalware.
- Enact multifactor authentication wherever possible.
- Ensure network segmentation.
- Disable RDP and other remoting options except when necessary.
- Keep software updated. Install software patches so that attackers can't take advantage of known problems or vulnerabilities.
- Conduct regular internet searches for student, faculty, and staff information to monitor its possible exposure and spread on the internet.

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 e-mail 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. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

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.

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