Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

1 June 2020

PIN Number
20200601-001

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 PIN was coordinated with DHS-CISA.

This PIN has been released **TLP: GREEN**: Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Cyber Threat to Law Enforcement and State Government Computer Systems Amid Civil Unrest

Summary

Due to ongoing civil unrest, hacktivist groups are actively threatening and endorsing cyber attacks against law enforcement and state government networks. The FBI is providing this Private Industry Notification to law enforcement partners to increase cyber vigilance and recommend mitigation to protect computer networks, outward facing webpages, and social media accounts against a cyber attack.

Threat

Hacktivist groups have historically conducted and advocated for cyber attacks following high-profile and controversial political or socioeconomic events. Groups such as “Anonymous” are actively leveraging societal and political unrest to encourage global cyber

action against law enforcement and government computer networks, outward facing web pages, and social media accounts. The FBI has identified active target lists published by individuals affiliating themselves with hacktivist groups, to include police departments and local and state government computer networks.

Historically, hacktivists have provided tools and guidance on cyber attack methodology and techniques to anyone willing to conduct an attack on behalf of their cause. Distributed denial of service attacks along with web page and social media profile defacement are a preferred tactic for hacktivist operations, but attackers have also conducted data exfiltration of emails and sensitive files for public release. Following the shooting of Michael Brown in 2014, individuals claiming affiliation with Anonymous attacked Ferguson City Hall's website and released personally identifiable information (PII) and personal family information for the St. Louis County police chief. Criminals used the PII to open fraudulent credit card accounts in the chief's name.

Hacktivist operations are conducted by sophisticated and non-sophisticated cyber actors globally, with followers receiving targets from individuals conducting extensive reconnaissance. Reconnaissance can include the use of web scanning tools to identify open network ports or unpatched vulnerabilities. This phase of activity can also target social media accounts of officers, government officials, and employees to create targeted phishing emails aimed at infecting networks through malicious attachments and links, creating an initial intrusion vector for follow-on cyber operations.

Recommended Mitigations

General Cyber Recommendations

- Update and patch all systems, to include operating systems, software, and any third-party code running as part of your website.
- Keep anti-virus and anti-malware up to date and firewalls properly configured.
- Create a disaster recovery plan to ensure successful and efficient communication, mitigation, and recovery in the event of an attack.

- Implement a password policy that requires passwords to be at least 14 characters or longer preferably using a passphrase to increase complexity while assisting user recall.

Email Phishing Recommendations

- Be wary of unsolicited attachments, even from people you know. Cyber actors can "spoof" the return address, making it look like the message came from a trusted associate.
- Keep software up to date. Install software patches so that attackers can't take advantage of known problems or vulnerabilities.
- If an email or email attachment seems suspicious, don't open it, even if your antivirus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the antivirus software might not have the signature.
- Save and scan any attachments before opening them.
- Turn off the option to automatically download attachments. To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and disable it.

Distributed Denial of Service Identification and Recommendations

- ***Identification***
  - Unusually slow network performance (opening files or accessing websites)
  - Unavailability of a particular website or the inability to access any website.

- ***Mitigation***
  - Enroll in a Denial of Service protection service that detects abnormal traffic flows and redirects traffic away from your network.
  - Create a partnership with your local internet service provider (ISP) prior to an event and work with your ISP to control network traffic attacking your network during an event.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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. 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.

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