Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

18 February 2016

Alert Number

160217-001

Please contact the FBI with any questions related to this PIN Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937
Local Field Offices:
www.fbi.gov/contact-us/field

Global Extremists Conducting Cyber Activity in Support of ISIL

Summary

Over the past 18-24 months, an unknown number of online extremists have conducted "hacktivist" cyber operations – primarily Web site defacements, denial-of-service attacks, and release of personally identifiable information (PII) in an effort to spread pro-Islamic State of Iraq and the Levant (ISIL) propaganda and to incite violence against the United States and the West. Recent open source reporting from the Daily Mail India, indicates ISIL is recruiting Indian hackers and offering upwards of $10,000 USD per job to hack government Web sites, steal data, and to build social media databases for recruiting purposes. Indian officials believe as many as 30,000 hackers in India may have been contacted. The FBI cannot confirm the validity of the media reports, and beyond this single article on Indian hackers and ISIL, does not have information indicating any such relationship exists to date. The FBI assesses this activity is most likely independent of ISIL's leaders located in Syria and Iraq.

Threat

The FBI has no information at this time that would identify any specific group or industry sector being targeted by pro-ISIL Web site defacements. We assess Web site vulnerabilities found using automated tools are the primary reason for target selection in past victims. Releases of PII, also known as doxing, by pro-ISIL hacktivists have primarily focused on U.S. and Western government personnel, especially military and law enforcement.

- Since at least August 2015, a group of pro-ISIL hackers calling themselves "Elite Islamic State Hackers," "Islamic Cyber Army," and "Caliphate Cyber Army" have been associated with multiple Web site defacements and PII releases. In September 2015, group members began posting a series of messages via

Twitter stating that they were conducting cyber attacks against the United States in commemoration of the September 11th terrorist attacks using the hash tag #AmericaUnderHacks for their Twitter postings. The postings included screenshots displaying access to several victim Web sites, as well as the posting of PII on President Barack Obama, the First Lady Michelle Obama, Congressional Staff members, government employees, and U.S. military members. Since the #AmericaUnderHacks hacking campaign in September 2015, group members have executed similar campaigns against the United Kingdom (#BritainUnderHacks), Saudi Arabia (#SaudiUnderHacks), Russia (#RussiaUnderHacks), and Israel (#IsraelUnderHacks).

- Open source reporting in India has noted the existence of several “hacking groups” within India. Thus far, such reporting has identified group names like “Indian Cyber Army” or “Shakti Campaign” and referenced such groups as having worked on behalf of the Indian government against Pakistan. To date, we have yet to see any validated reporting as to the capabilities of such groups or been able to confirm their existence. It does stand to reason; however, criminal hacking activity, whether by individuals or from organized groups exists in India and could potentially target US companies both for financial gain and for general acclaim.

Technical Details

The FBI assesses most pro-ISIL hacktivist groups use relatively unsophisticated methods and tools to scan for and exploit well-known Web site vulnerabilities. Structured Query Language (SQL) injection, Cross Site Scripting (XSS), and social engineering tactics to obtain account credentials are assessed to be in the capability range of pro-ISIL cyber actors.

The recruited Indian hackers are reportedly communicating on Internet based services like Skype, Silent Circle, Telegram, and WhatsApp. Pro-ISIL hackers use social media platforms like Twitter to make public announcements and release PII. Larger PII releases have been uploaded to online text sharing sites such as Pastebin.com and Justpaste.it.

Defense

Precautionary measures to mitigate computer intrusion threats include:

- Enable automated patches for common vulnerabilities, and routinely update hardware and software applications, including anti-virus software.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software from sites you know and trust.
- Disable macros. Be careful of pop-ups from attachments that require you to enable them.

- Monitor employee logins that occur outside of normal business hours.
- Avoid using the same login and password for multiple platforms, servers, or networks.
- Use two-factor authentication for employee logins, especially remote logins.
- Create a centralized Information Technology email account for employees to report suspicious emails.
- Provide regular training to remind and inform employees about current social engineering threats.
- Monitor unusual traffic, especially over non-standard ports; and close unused ports.
- Monitor outgoing data, and be willing to block unknown IP addresses.
- Utilize a Virtual Private Network (VPN) for remote login capability.

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 e-mail at CyWatch@ic.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@ic.fbi.gov or 202-324-3691.

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as for peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

There is no additional information available on this topic at this time. For comments or questions related to the content or dissemination of this product, please contact CyWatch.