Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

30 March 2015

PIN Number
PIN 150330-001

Please contact the FBI with any questions related to this PIN 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

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and systems administrators to guard against national security and criminal cyber threats.

Pending Anti-Israeli Hacktivist Operation Could Potentially Impact US Systems

General Observations

As of early March 2015, several extremist hacking groups indicated they would participate in a forthcoming operation, #OpIsrael, which will target Israeli and Jewish Web sites. The FBI assesses members of at least two extremist hacking groups are currently recruiting participants for the second anniversary of the operation, which started on 7 April 2013, and coincides with Holocaust Remembrance Day. These groups, typically located in the Middle East and North Africa, routinely conduct pro-extremist, anti-Israeli, and anti-Western cyber operations.

While the threat to US-based infrastructure is assessed as low for well-maintained and updated systems, the FBI is using the Private Industry Notification (PIN) as a method of notifying possible targeted entities.

FBI and private cybersecurity industry analysis of previous extremist hacker campaigns and operations indicate these groups are capable of low-level Distributed Denial of Service (DDoS)[1] attacks and Web site defacements. The most likely targets for the campaign are Israel-based systems or the systems of worldwide Jewish-oriented organizations like synagogues or cultural centers. Based on historical targeting preferences, the attackers will likely focus primarily on Israeli financial institutions, but may also target Israeli media outlets.

[1] A type of denial-of-service attack in which an attacker uses malicious code installed on multiple computers to attack a single target.

Given the perceived connections between the Government of Israel and Israeli financial institutions, and those of the United States, #OpIsrael participants may also shift their operations to target vulnerable US-based financial targets or Jewish-oriented organizations within the United States. Based on historical attacks, the FBI assesses that attacks which may spawn from #OpIsrael to target US-based systems will likely constitute only a small percentage of overall activity.

The FBI assesses Web site defacements are the most likely method by which #OpIsrael participants will be successful against their targets. While most Web sites maintain up-to-date content management software, the ease with which attackers can exploit known or un-patched vulnerabilities makes this the more likely vector. Sites which maintain updated systems will not likely be impacted by defacement operations.

The FBI assesses most DDoS attempts made by #OpIsrael actors will have little to no effect on targeted Web sites, due to traditionally disorganized attacks, and existing DDoS mitigation measures in-place by potential victims. Historically, anti-Israel DDoS operations have failed to gain significant traction given competing priorities for the groups and individuals involved, and the limited number of participants who could organize to conduct successful DDoS campaigns.

Defense

In general, extremist hacktivism cyber attacks may result in denial of service, defacement of a Web site, and compromise of sensitive information, which may lead to harassment and identity theft. Precautionary measures to mitigate a range of potential extremist hacktivism cyber threats include:

- 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.
- Scrutinize links contained in email attachments.
- Regularly mirror and maintain an image of critical system files.
- Encrypt and secure sensitive information.
- Use strong passwords, implement a schedule for changing passwords frequently, and avoid reusing passwords for multiple accounts.
- Enable network monitoring and logging where feasible.
- Be aware of social engineering tactics aimed at obtaining sensitive information.
- Securely eliminate sensitive files and data from hard drives when no longer needed or required.
- Establish a relationship with local law enforcement and participate in IT security information sharing groups for early warning of threats.

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@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 with 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, contact CyWatch.