FBI Cyber Division

Private Industry Notification

DATE: 24 September 2014

PIN #: 140924 – 001

(U) Threat of Cyberterrorist and Hacktivist Activity in Response to US Military Actions in the Middle East

(U) General Observations:

(U//FOUO) The FBI has no information at this time to indicate specific cyber threats to US networks or infrastructure in response to ongoing US military air strikes against the terrorist group known as the Islamic State of Iraq and the Levant (ISIL), also known as the Islamic State of Iraq and al-Shams (ISIS) or the Islamic State (IS). However, the FBI assesses extremist hackers and hacktivist groups, including but not limited to those aligned with the ISIL ideology, will continue to threaten and may attempt offensive cyber actions against the United States in response to perceived or actual US military operations in Iraq or Syria. The FBI bases this assessment on recent, nonspecific, and probably aspirational threats made on social media platforms to carry out cyber as well as physical attacks in response to the US military presence in the Middle East.

- (U//FOUO) In mid-May 2014, the hacktivist group Tunisian Hackers Team threatened Distributed Denial of Service (DDoS) attacks against the US financial sector unless US military forces were withdrawn from presumed-Islamic lands (for additional information, see PIN# 140624-015).

- (U) As of early-2014, Twitter user @AnonArabOps expressed support for ISIL, provided guidance on the use of various hacking tools, and called for cyber attacks against the United States and Israel.

- (U) As of early-September 2014, a British media outlet identified the hacker known as Abu Hussain Al Britani as a Syria-based ISIL fighter. Al Britani previously served a six-month sentence in the United Kingdom for hacking the e-mail account of former Prime Minister Tony Blair, according to the media report.

- (U) On 7 September 2014, Twitter user @Dawlamoon posted messages encouraging attacks against Twitter employees, likely in response to Twitter's takedown of several pro-ISIL accounts.

(U) Impact:

(U//FOUO) Middle East-based hacktivist groups and extremist cyber actors have previously targeted US commercial and government Web sites in response to a range of US military actions

and foreign policy positions. Analysis by the FBI and the private cyber security industry suggests that the most likely tactics, techniques, and procedures utilized by these groups are Cross Site Scripting (XSS), Structured Query Language (SQL) Injection, and TCP/UDP Flooding for defacement and DDoS attacks. Web site defacements conducted by these actors will likely contain messages expressing support for ISIL, and/or contain imagery such as the black ISIL flag (Figure 1) or graphic imagery, e.g., pictures or videos of ISIL executions.

(U) Figure 1: ISIL Flag

(U) Defending Against Hacktivism

(U//FOUO) In general, 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. Although the specific claims referenced above do not speak specifically to a particular attack vector, precautionary measures to mitigate a range of potential hacktivism threats include:

- (U//FOUO) 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.
- (U//FOUO) Have a DDoS mitigation strategy ready ahead of time and keep logs of any potential attacks.
- (U//FOUO) Scrutinize links contained in e-mail attachments.
- (U//FOUO) Regularly mirror and maintain an image of critical system files.
- (U//FOUO) Encrypt and secure sensitive information.
- (U//FOUO) Use strong passwords, implement a schedule for changing passwords frequently and do not reuse passwords for multiple accounts.
- (U//FOUO) Enable network monitoring and logging where feasible.
- (U//FOUO) Be aware of social engineering tactics aimed at obtaining sensitive information.
- (U//FOUO) Securely eliminate sensitive files and data from hard drives when no longer needed or required.
- (U//FOUO) Establish a relationship with local law enforcement and participate in IT security information sharing groups for early warnings of threats.

(U) There is no additional information available on this topic at this time.

(U) Reporting Notice:

(U//FOUO) The FBI and US-CERT encourage recipients of this document to report information concerning suspicious or criminal activity to your local FBI field office. The FBI's 24/7 Cyber Watch (CyWatch) can be reached by telephone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. US-CERT can be reached by telephone at 888-282-0870 or by e-mail at SOC@us-cert.gov. The US-CERT homepage can be found online at www.us-cert.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.

(U) Administrative Note

(U) 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.