Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

November 18, 2015

Alert Number
**I-042115(Revised)-PSA**

# HACKTIVISTS THREATEN TO TARGET LAW ENFORCEMENT PERSONNEL AND PUBLIC OFFICIALS

### Summary

Law enforcement personnel and public officials may be at increased risk of being targeted by hacktivists. Hacking collectives are effective at leveraging open source, publicly available information identifying officers and public officials, their employers or associates, and their families. With this in mind, officers and public officials should be highly aware of their email account security and their online presence and exposure. For example, posting images wearing uniforms displaying name tags or listing their police department on social media sites can increase an officer's risk of being targeted or attacked.

Many legitimate online posts are linked directly to personal social media accounts. Law enforcement personnel and public officials need to maintain an enhanced awareness of the content they post and how it may reflect on themselves, their family, and their employer, or how it could be used against them in court or during online attacks.

### Threat

In a recent threat, a threat actor typically contacts the Internet Service Provider (ISP) of the target, poses as an employee of the company, and requests details regarding the target's account. Utilizing these details, the caller then contacts the target's email provider, successfully provides answers to security questions established for the email account, and is granted a password reset for the account. Ultimately, the actor gains access to the victim’s email account and begins to harvest personal or other information.

Threat actors may also target law enforcement personnel and public officials through doxing. Doxing is the act of compiling and posting an individual's personal information without permission. The personal information gathered from social media and other Web sites could include home addresses, phone numbers, email addresses, passwords, and any other information used to target an individual during a cyber attack. The information is then posted on information-sharing Web sites with details suggesting why the individual should be targeted.

Recent activity suggests family members of public officials and law enforcement officers are also at risk for these types of targeting activity. Targeted information may include personally identifiable information and public information and pictures from social media Web sites.

### Defense

While eliminating your exposure in the current digital age is nearly impossible, law enforcement officers and public officials can take steps to minimize their risk in the event they are targeted.

- Enable additional email security measures, including two-factor authentication on your personal email accounts. This is a security feature offered by many email providers. The feature will cause a text message to be sent to your mobile device prior to accessing your email account.

- Turn on all privacy settings on social media sites and refrain from posting pictures showing your affiliation to law enforcement.

- Carefully evaluate the user settings for your online profiles. The default settings for some sites may allow anyone to see a user’s profile. Settings can be customized to restrict access to certain people.

- Keep your social media footprint to a minimum, where possible, and actively monitor any accounts you maintain.

- When posting on social media sites, do not provide details regarding your workplace, work associates, official position, or duties.

- Do not promote your personal or professional importance in online profiles or postings, as this may make you a potential target for adversaries to exploit.

- Limit your personal postings on media sites and carefully consider your comments.

- Be aware of your security settings on your home computers and wireless networks.

- Routinely update hardware and software applications, as old versions may be exploited by criminals as a way to access a computer. In addition, maintain up-to-date antivirus software, as attackers are continually writing new viruses.

- Pay close attention to all work and personal emails, especially those containing attachments or links to other Web sites. These suspicious or phishing emails may contain infected attachments or links.

- When setting up security questions for any of your accounts, avoid choosing questions with answers that can be easily verified (e.g., "What is your mother's maiden name?"). Devise questions and answers that are known only to you. If the questions are already provided, devise answers known only to you. Try using secret meanings, irony, metaphors, or even "incorrect" responses that no one but you would be able to guess.

- Passwords should be changed regularly. It is recommended that you create a password phrase of 15 characters or more, using a combination of uppercase and lowercase letters, numbers, symbols, and special characters.

- Do not store your login credentials on or near your computer. Memorize them or store them in a secure location away from your devices.

- Be aware of pretext or suspicious phone calls or emails from people phishing for information or pretending to know you. Social engineering is a skill often used to trick you into divulging confidential information and continues to be an extremely effective method for criminals.

- Advise family members to turn on security settings on ALL social media accounts. Family member associations are public information and family members can become online targets of opportunity.

- Restrict your driver license and vehicle registration information with the Department of Motor Vehicles.

- Request real estate and personal property records be restricted from online searches with your specific county.

- Closely monitor your credit and banking activity for fraudulent activity.

- Routinely conduct online searches of your name to identify what public information is already available.