Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

April 21, 2015

Alert Number
I-042115-PSA

HACKTIVISTS THREATEN TO TARGET LAW ENFORCEMENT PERSONNEL AND PUBLIC OFFICIALS

Summary

Law enforcement personnel and public officials may be at an increased risk of cyber attacks. These attacks can be precipitated by someone scanning networks or opening infected emails containing malicious attachments or links. Hacking collectives are effective at leveraging open source, publicly available information identifying officers, their employers, and their families. With this in mind, officers and public officials should be aware of 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, their employer or how it could be used against them in court or during online attacks.

Threat

The act of compiling and posting an individual's personal information without permission is known as doxing. 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 law enforcement personnel and public officials are also at risk for cyber attacks and doxing activity. Targeted information may include personally identifiable information and public information and pictures from social media Web sites.

Another dangerous attack often used by criminals is known as “swatting.” This involves calling law enforcement authorities to report a hostage situation or other critical incident at the victim's residence, when there is no emergency situation.

Defense

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

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

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

	• Limit your personal postings on media sites and carefully consider comments. • 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. • Routinely update hardware and software applications, including antivirus. • 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. • Routinely conduct online searches of your name to identify what public information is already available. • Enable additional email security measures to include 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. • Closely monitor your credit and banking activity for fraudulent activity. • Passwords should be changed regularly. It is recommended to use a password phrase of 15 characters or more. Example of a password phrase: Thisisthemonthofseptember,2014. • 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.