ROLL CALL RELEASE
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SHARING PERSONNEL

24 March 2016

(U) ISIL Supporters Compromise of Law Enforcement Personal Data for Possible Targeting

(U//FOUO) Individuals supporting the Islamic State of Iraq and Levant (ISIL), who in 2015 began posting personally identifiable information (PII) of US military and federal employees to ISIL-affiliated social media accounts, are expanding their targeting to include law enforcement (LE) officers, according to US media reporting.[2,3,4] ISIL is using the technique known as "doxing" to release personal information to the public to harass targeted individuals and possibly to provide sympathizers who could be willing to conduct attacks with information that would assist them in targeting military, LE officers, and federal personnel. ISIL has consistently called for attacks against military, intelligence, and LE personnel in its public English-language messaging, and supporters may view attacking these specific individuals as sanctioned by the group.

UNCLASSIFIED

(U) Caliphate Cyber Army (CCA)[1]

» (U) Individuals reportedly affiliated with the pro-ISIL Caliphate Cyber Army (CCA) hacking group on 15 March 2016 posted a "kill list" on social media, with full identifying information on 36 police officers living in Minnesota, according to US media reporting.[5] The FBI is investigating threatening phone calls to LE officials, possibly resulting from these CCA postings. This is a direct threat to LE officers from pro-ISIL hackers. A member of CCA on 2 March 2016 posted a video to social media showing the alleged hack of a Midwestern police association, according to media reporting.[6] The hack included dissemination of contact information on association members and defacing the association's website, according to the same US media reporting.[7]

» (U) The CCA member posting the video of the police association compromise, using the @hackcca social media account, on 2 March 2016 also posted PII of 50 police officers from New Jersey, according to a DHS fusion center intelligence officer.[8] The PII included their names, home and work addresses, and phone numbers, according to the same DHS intelligence officer.[9]

» (U) A Kosovar citizen, Ardit Ferizi, was detained in Malaysia in early fall 2015 after reportedly hacking into a US web hosting company and extracting PII of over 1,300 US military and federal personnel, according to a computer security blog.[10] He subsequently passed this information to an ISIL member who posted the PII to social media accounts, with the expressed desire for sympathizers to target and kill the identified personnel, according to the same blog report.[11]

(U) US-CERT Best Practices to Avoid Data Compromises[12]

- (U) Limit the amount of personal information you post.
- (U) Remember that the Internet is a public resource.
- (U) Be wary of strangers or persons out of the norm contacting you on social media and requesting personal information.
- (U) Evaluate your settings and limit access to your information.
- (U) Use strong passwords on all accounts.
- (U) Check privacy policies and limit options for individuals viewing your social media account.

(U) DHS's Computer Emergency Readiness Team, commonly known as US-CERT, has many helpful resources describing techniques to apply when posting information on social networking websites, including "Staying Safe on Social Networking Sites" (https://www.us-cert.gov/ncas/tips/ST06-003) and "Socializing Securely: Using Social Networking Services" (https://www.us-cert.gov/security-publications/socializing-securely-using-social-networking-services). Additionally, the FBI's Internet Crime Complaint Center, or IC3 has issued alerts about doxing of LE personnel and other public officials.

(U) Report Suspicious Activity

(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.

---

[1] (U); Gilad Shiloach; Vocativ; ISIS Hackers Post "Wanted" List Of Minnesota Cops; 14 MAR, 2016; http://www.vocativ.com/news/296718/isis-hackers-post-wanted-list-of-minnesota-cops; accessed on 15 MAR 2016.

[2] (U); P.H. Madore; Hacked.com; "ISIS Has Allegedly Doxed 100 US Military Personnel"; 23 MAR 2015; https://hacked.com /isis-allegedly-doxed-100-us-military-personnel/; accessed on 09 MAR 14.

[3] (U); John Zorabedian; Naked Security; "Hacker detained for giving US service members' personal info to ISIS"; 17 Oct 2015; https://naked security.sophos.com/2015/10/17/hacker-detained-for-giving-us-service-members-personal-info-to-isis/; accessed on 09 MAR 14.

[4] (U); Gilad Shiloach; Vocativ; ISIS Hackers Post "Wanted" List Of Minnesota Cops; 14 MAR, 2016; http://www.vocativ.com/news/296718/isis-hackers-post-wanted-list-of-minnesota-cops; accessed on 15 MAR 2016.

[5] (U); Gilad Shiloach; Vocativ; ISIS Hackers Post "Wanted" List Of Minnesota Cops; 14 MAR, 2016; http://www.vocativ.com/news/296718/isis-hackers-post-wanted-list-of-minnesota-cops; accessed on 15 MAR 2016.

[6] (U); Memri Cyber and Jihad Lab; "Caliphate Cyber Army Hacks U.S. Police Website"; 02 MAR 2016; http://cjlab.memri.org/uncategorized /caliphate-cyber-army-hacks-u-s-police-website/; accessed on 10 MAR 2016.

[7] (U); Memri Cyber and Jihad Lab; "Caliphate Cyber Army Hacks U.S. Police Website"; 02 MAR 2016; http://cjlab.memri.org/uncategorized /caliphate-cyber-army-hacks-u-s-police-website/; accessed on 10 MAR 2016.

[8] (U); DHS; NYC, Senior Intelligence Officer; E-mail; 02 MAR 2016; DOI 02 MAR 2016; (U); FYSA: NJ Transit PD; Extracted information is Unclassified; Overall document classification is UNCLASSIFIED.

[9] (U); DHS; NYC, Senior Intelligence Officer; E-mail; 02 MAR 2016; DOI 02 MAR 2016; (U); FYSA: NJ Transit PD; Extracted information is Unclassified; Overall document classification is UNCLASSIFIED.

[10] (U); John Zorabedian; Naked Security; "Hacker detained for giving US service members' personal info to ISIS"; 17 Oct 2015; https://naked security.sophos.com/2015/10/17/hacker-detained-for-giving-us-service-members-personal-info-to-isis/; accessed on 09 MAR 14.

[11] (U); John Zorabedian; Naked Security; "Hacker detained for giving US service members' personal info to ISIS"; 17 Oct 2015; https://naked security.sophos.com/2015/10/17/hacker-detained-for-giving-us-service-members-personal-info-to-isis/; accessed on 09 MAR 14.

[12] (U); US-CERT; Security Tip ST06-003; Staying Safe on Social Networking Sites; https://www.us-cert.gov/ncas/tips/ST06-003; accessed on 10 MAR 2016.