NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | *September 16, 2015*

Threat Indicators

ISIS-Symphathizers Continue to Deface Websites

Earlier this week, the FBI issued an update to a **TLP: GREEN** alert regarding the recent activity of an ISIS-symphathetic hacking group, known as the "Islamic Cyber Army" (ICA), related to the anniversary of the September 11, 2001 terrorist attacks. The ICA group, and other ISIS-inspired hacktivists, are likely to continue conducting website defacements by exploiting targets of opportunity, as well as the unauthorized release of US citizens' personally identifiable information (PII), known as doxing. For more information and technical indicators related to the ICA group, please contact the NJCCIC.

Tip of the Week

"Managing Your Digital Footprint"

Once information is online, sometimes it can be impossible to remove. You should be conscientious of your visible online presence

Latest Cyber Alerts

[Secret Mobile Apps](#)

NJ CyberLog

[Vehicle Cybersecurity: Industry Responds to Vulnerabilities](#)

A series of media reports throughout the summer drew attention to various vulnerabilities in many of today's Internet-connected vehicles. While the identified security gaps present serious risks to public safety and certainly warrant an industry-wide response, it is important to note that there have since been no reports of malicious hijacking of a vehicle's vital functions by a cyber threat actor. Nonetheless, these disclosures underscore an overall lack of cybersecurity considerations as more of our lives are connected to the 'Internet of Things'. As with the tech industry, auto manufacturers are striving to innovate and be the first to market with the next best thing; however, the abundance of integrated computers and Internet-connected add-ons are sacrificing the security of their users (or in the case of cars, their passengers).

known as your digital footprint, as criminals and fraudsters may utilize this information against you in various ways. The more information out there, the more information that is accessible for social engineering and ID theft scams.

Be cautious of what you post online and take the following steps below to manage your digital footprint!

Recommendations:

1. Map your digital footprint. Look at all the social networking sites and forums that you belong to and search what information about you is available.
2. Clean up your digital footprint. Remove any photos, content and links that may be inappropriate or reveal too much information.
3. Be selective about who you authorize to access your information.
4. Use the privacy features of your browser and of the various websites you frequent to reduce the visibility of your information.
5. Think before you post.

NJCCIC Announcements

The Critical Infrastructure Cybersecurity (C3) Voluntary Program, NJOHSP and NJCCIC Regional Cybersecurity Event starts today! Details on how to tune in if you are not registered or unable to attend:

Today, Sept. 16: 2:00pm - 4:30pm
Tomorrow, Sept. 17: 9:00am - 3:45pm

Virtual Conference Information:

Dial-In: 888-251-2909
PIN: 5107327#

AT&T Connect Link

Prepare in advance

Supported Operating Systems and Devices

Questions?

Email a Cyber Liaison Officer at

njccic@cyber.nj.gov

Connect with us!

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

Share this email: