NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | January 22, 2016

Cyber-Terrorism: A Growing Threat

The NJCCIC contributed a short assessment on cyber-terrorism for the recently released Terrorism Threat Assessment 2016 from the New Jersey Office of Homeland Security and Preparedness (NJOHSP). ***We assess the cyber threat to New Jersey from terrorist groups is low despite their intent to target the United States.***


UNCLASSIFIED

NJOHSP
OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

Cyber-Terrorism: A Growing Threat

The cyber threat to New Jersey from terrorist groups is low despite their intent to target the United States. According to the FBI, terrorist organizations, including ISIS, al-Qa'ida, and Hizballah, are attempting to build offensive cyber capabilities, but to date they have had little to no success.

- In October, a media report citing federal sources indicated ISIS had attempted—unsuccessfully—to gain access to the US electric grid.

Terrorist groups are likely to continue developing cyber capabilities and will attempt disruptive or destructive cyber attacks as a means of intimidation and coercion. We assess ISIS is the most likely terrorist group to attempt cyber operations against US resources, but its capabilities remain limited to low-level activities such as socially engineered account compromises and website defacements.

- In August, Junaid Hussain, a British citizen reportedly responsible for leading cyber operations and recruitment for ISIS, was killed in Syria. Hussain allegedly released US service members' personal information last year—a tactic known as "doxing"—and used social media to inspire terrorist attacks in the West.

ISIS could leverage international hackers with more advanced cyber capabilities. These hackers often exploit targets of opportunity such as organizations with weak cybersecurity defenses. Large and thriving online black marketplaces, where off-the-shelf hacking tools and capable hackers offer intrusion or attack services for nominal fees, could also be utilized.

- In October, a Malaysia-based hacker was arrested on a provisional US arrest warrant alleging he hacked a US company's servers, stole personal information of 1,300 US military and federal personnel, and provided the data to ISIS, which subsequently released it on social media.

Terrorists Using Encryption Technology

The widespread proliferation of peer-to-peer (P2P) encryption technology has helped terrorists shield their communications from conventional surveillance techniques, creating digital safe havens for operational planning, command and control, logistics, and execution. Beyond the cryptographic challenges of surveilling this terrorist traffic, most technology companies lack access to terrorists' private encryption keys to unlock data in compliance with lawful search warrants.

This portion of the assessment was produced by the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC). Visit www.cyber.nj.gov to learn more.

UNCLASSIFIED

We assess ISIS is the most likely terrorist group to attempt cyber operations against US resources, but its capabilities remain limited to low-level activities such as socially engineered account compromises and website defacements.

Click here for the full Threat Assessment.

NJCCIC Blog Follow-up: Passwords

In our previous blog post, "Passwords, Passwords, Passwords", we stressed the importance of passwords and provided some practical guidance for how to create and remember strong passwords. For the last five years, a software vendor by the name

Latest Cyber Alerts

Multiple Vulnerabilities in Cisco Products Could Allow for Unauthenticated, Remote Access

Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (Updated)

Multiple Vulnerabilities in PHP Could Allow Arbitrary Code Execution (Updated)

of SplashData has compiled a list of the most commonly used "worst" passwords, aggregated from the previous year's data breaches. For the fifth year in a row, "123456" and "password" were the two most commonly occurring out of the more than two million passwords analyzed. If you use one of the 25 on the list, please revisit our blog or the check out the "10 simple rules" from cybersecurity firm Kaspersky.

Tip of the Week

" Safeguards for 2016"

Because of improved protections in recent years, the Internal Revenue Service (IRS) stops the vast majority of fraudulent tax returns using stolen identities. But identity thieves and criminal syndicates continue to persist and evolve.

Read more about this cyber tip and others from the IRS

Cyber News

Cyber-attack among World Economic Forum's top global risks
via SC Magazine

Both public and private sectors 'blind' to cyber risk
via FedScoop

Chinese soldiers implicated in U.S. military hacking case
via the Globe and Mail

Firm Sues Cyber Insurer Over $480K Loss
via Krebs on Security

The Lowdown on Freezing Your Kid's Credit
via Krebs on Security

Ukrainian power companies are getting hit with more cyberattacks
via CSO Online

Critical Updates for Apple, Linux, and Oracle

The NJCCIC strongly recommends users of the following software apply updates immediately.

Apple: On Tuesday, Apple released security updates for iOS, OS X, and Safari, patching thirteen vulnerabilities. Many of these vulnerabilities could allow remote code execution, providing attackers access to a device and the ability to then execute malicious code or gain complete control of the compromised device. Victims can be impacted merely by visiting a malicious website. Technical details and updates available here.

Linux: On Tuesday, Linux issued a source code patch to address a critical Linux kernel vulnerability. The flaw has been present in the code since 2012, and also extends to two-thirds

of Android devices. A compromised device can provide an attacker root level access and the ability to execute code. A patch is available as source code; however, Red Hat has not issued a patch as of January 20. Technical details and updates available here.

Oracle: On Tuesday, Oracle issued patches to 248 new vulnerabilities affecting multiple Oracle products. Many of these vulnerabilities could be remotely executed by attackers. Oracle is receiving reports that malicious actors have attempted and successfully exploited these vulnerabilities. Technical details and updates available here.

Questions?

Email a Cyber Liaison Officer at
njccic@cyber.nj.gov.

Connect with us!

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell