NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | February 12, 2016

Ransomware - An Enduring Risk for Organizations and Individuals

The NJCCIC assesses with high confidence that many businesses, schools, government agencies, and home users will remain at high risk of ransomware infections throughout 2016, as financially-motivated hackers continue to innovate and expand the targeting scope of their extortion campaigns. The observed increase in ransomware infections and development of new variants over the last two years illustrates the attractive incentives for criminal hackers, as the perceived return on investment outweighs the risk of attribution and prosecution. In recent months, numerous cybersecurity firms released threat predictions for 2016, with universal agreement that ransomware and other forms of cyber extortion would not only continue to increase, but expand into new digital territories. For more, read our full threat analysis.

Cyber Blog

Tax Scams and Identity Theft: What You Need to Know

By now, you should have received all of the necessary forms and paperwork required to complete your 2015 tax returns. This year, though, you may not want to wait until the last minute to file your taxes, lest an identity thief tries to beat you to the punch to steal your refund. Believe it or not, the IRS paid out an estimated $5.8 billion in fraudulent tax refunds in 2013. To find out how to prevent yourself from falling victim to tax scams and identity theft, read the full blog post.

Breach Notification

Department of Justice (DoJ)

On Monday, an anonymous hacker using the

Latest Cyber Alerts

Buffer Overflow Vulnerability in Cisco ASA Software Products Could Allow for Remote Code Execution

Twitter handle @DotGovs released the names, titles, phone numbers, and email addresses of over 9,000 DHS and 20,000 FBI personnel. The DoJ is investigating after the hacker's claim of compromising DoJ systems in order to obtain the data. If you would like to confirm whether or not your information was released, please contact the NJCCIC.

Internal Revenue Service (IRS)

On Tuesday, the IRS announced it had identified and halted an automated attack upon its Electronic Filing PIN application on IRS.gov. Identity thieves used malware and 101,000 SSNs stolen from outside of the IRS to successfully generate E-file PINs. The IRS stated that no personal taxpayer data was compromised or disclosed by IRS systems; however, affected taxpayers will be notified by mail that their personal information was used in an attempt to access the IRS application.

Gyft Inc.

The gift card provider Gyft acknowledged there was unauthorized access to two of their cloud providers between October 3 and December 18, 2015. The unauthorized party was able to view or download certain user information, including names, addresses, dates of birth, phone numbers, email addresses, and gift card numbers. The gift card numbers could have been used to make unauthorized purchases. In addition, the log-in credentials for anyone who attempted to use Gyft between March 19 and December

Multiple Vulnerabilities in Adobe Products Could Allow for Remote Code Execution

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

Vulnerability in Microsoft Windows Journal Could Allow for Remote Code Execution

Security Update for Microsoft Office to Address Remote Code Execution

Vulnerabilities in Microsoft Windows PDF Library Could Allow for Remote Code Execution

Cumulative Security Update for Microsoft Edge

Cumulative Security Update for Internet Explorer

Cyber In The News

The President's National Cybersecurity Plan: What You Need to Know

via The White House Blog

The Research Pirates of the Dark Web

via The Atlantic

The Black Market for Netflix Accounts

via The Atlantic

Gmail to warn when email comms are not encrypted

via Help Net Security

Southwest Airlines flight giveaway scams

4, 2015 may have been compromised. Victims may call 866-287-0504 for more information.

spread on Facebook

via We Live Security

White House Releases Cybersecurity National Action Plan

On Tuesday, the White House announced a new Cybersecurity National Action Plan (CNAP) to "enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security."

Highlights of the CNAP include actions to:

- Establish the “Commission on Enhancing National Cybersecurity”
- Propose a $3.1 billion Information Technology Modernization Fund to modernize government IT
- Empower Americans to secure their online accounts with best practices such as two-factor authentication (2FA)
- Invest over $19 billion for cybersecurity as part of the President’s Fiscal Year (FY) 2017 Budget

For more information, check out this CNAP Fact Sheet on WhiteHouse.gov.

Worldwide Threat Assessment of the U.S. Intelligence Community

On Tuesday, the Director of National Intelligence, James Clapper, and the Director of the Defense Intelligence Agency, Lieutenant General Vincent Stewart, delivered testimony to the Senate Armed Services Committee on the Intelligence Community's assessments of various global threats. The full Statement for the Record is available here.

For the third year in a row, the report leads off with cyber and technology threats - a strong indication of the national security implications of both state and non-state cyber operations. Here are some key takeaways:

- Russia and China remain our most sophisticated cyber adversaries, and continue to target the United States and our allies.
- Iran and North Korea also remain capable and willing actors, likely to continue cyber operations to support their political objectives.
- Cyber criminals remain the most pervasive threat to the US financial sector, using cyber to conduct theft, extortion, and other criminal activities.
- Rapid growth of the 'Internet of Things' and ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems.
- Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity to affect decisionmaking, reduce trust in systems, or cause adverse physical effects.

Questions?

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

Connect with us!

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

communications@njohsp.gov
Trenton, NJ | 08625 US