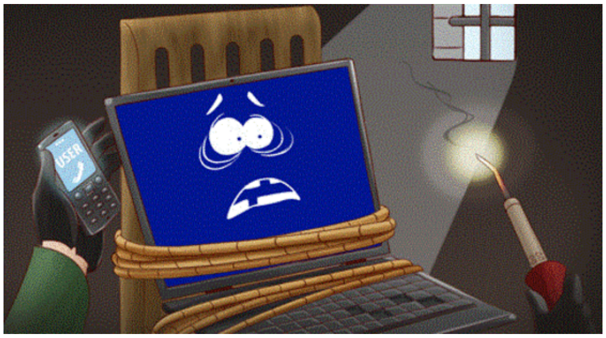
NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | February 26, 2016

Cyber Blog



What You Don't Know Can Cost You

The NJCCIC has been talking a lot about the topic of cyber extortion lately, and with good reason. Just two months into 2016, there have already been a number of cyber extortion attacks across the country, impacting all kinds of individuals, businesses, and organizations. We don’t see this trend subsiding any time soon, because more and more criminals are discovering that it’s a quick and effective way to make a lot of money in a short amount of time. With a myriad of free and low-cost tools at their disposal, these profit-motivated, tech-savvy criminals are able to easily launch an extortion campaign against their victims knowing the potential rewards far outweigh the risk of getting caught. For more on cyber extortion attacks, read the full blog post.

NJCCIC *at a glance*

Baltimore Hackers Say They Reveal Potentially Deadly Cybersecurity Weaknesses at Area Hospitals

NJCCIC Comment: A two-year investigation conducted by Independent Security Evaluators concluded that "patient health remains extremely vulnerable" throughout the healthcare sector as a result of the "lack of executive support, insufficient talent, improper implementations of technology, outdated understanding of adversaries, lack of leadership, and a misguided reliance upon compliance.” Although their efforts focused on facilities in the Baltimore and Washington areas, we assess the shortcomings and recommended actions apply industry-wide.

Report: 2016 Phishing Trends Reveal New Tricks, Targets

NJCCIC Comment: The report from NetworkWorld found that the United States accounted for 77 percent of phishing attacks in 2015, and business email compromise spear-phishing saw the biggest increase in 2015. The NJCCIC assesses email-based threats are the most common, yet avoidable, threat facing our members.

Zika Virus Outbreak Concerns Used to Spread Malware

NJCCIC Comment: Cybercriminals often capitalize on newsworthy events that are likely to pique curiosity or evoke an emotional response by crafting enticing phishing emails which can help deliver a malicious payload to their victims' systems or mobile devices. It is important to stay alert and always verify the sender of an unexpected email before taking any further action.

uKnowKids: Website Exposes Names and Images of Thousands of Children

NJCCIC Comment: Hacks like these are a good reminder, especially to parents, that anything connected in one way or another to the Internet is potentially vulnerable to compromise.

Tip of the Week

"Remain Vigilant Against Tax-Related Scams"

The IRS issued an advisory stating that reports of email and text-based scams were up 400 percent this year, a figure that is expected to increase in the lead-up to the April 15 tax deadline. There were 1,026 incidents reported in January, compared to 254 in 2015.

Be suspicious of all tax-related emails and text messages that request personally identifiable information, account credentials, or tax return information, or ask you to click a link to update your information. Scammers will use this information to fraudulently claim tax refunds before the victims has submitted their tax returns. Generally, the

Latest Cyber Alert

Linux Mint Website Hacked – Malicious ISO Files and Compromised Forums Database

DHS Webinar

Cybersecurity in the Health and Public Safety Sectors

Join this discussion to learn how our Nation's health and safety sectors are integrating cybersecurity measures, including the National Institute of Standards and Technology (NIST) Cybersecurity

IRS does not initiate contact with taxpayers by email or text message to request personal or financial information.

Tax preparers are also being targeted through spear-phishing emails in attempts to obtain the target's Preparer Tax Information Number (PTIN), providing access to the IRS filing system.

Framework, into their comprehensive enterprise risk management. Click here for additional information about this webinar.

Questions?

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

Connect with us!

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

DISCLAIMER: This bulletin is provided as is for informational purposes only. The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) and the Regional Operations Intelligence Center (ROIC) do not provide any warranties of any kind regarding any information contained within. The NJCCIC and ROIC do not endorse any commercial product or service, referenced in this bulletin or otherwise. Further dissemination of this bulletin is governed by the Traffic Light Protocol (TLP). For more information about TLP, see https://www.us-cert.gov/tlp/.