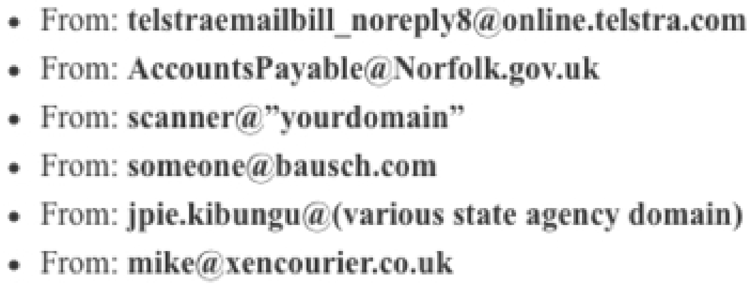
NJCCIC

NJ Cybersecurity & Communications Integration Cell

The Weekly Bulletin | November 20, 2015

Alert: Dridex Phishing Campaigns

The NJCCIC has observed a steady increase in Dridex malware. This week, our Operations Branch detected six highly effective Dridex phishing campaigns directed at State agencies. Dridex is a trojan designed to steal user credentials and attempt to obtain funds from banking services. The best practice to mitigate this threat is to educate all users on safe email and internet practices, most importantly, to never click on links or download attachments from unsolicited emails or messages from unknown senders. Users should be trained to carefully scrutinize all email and immediately report suspicious messages or online activity to IT staff. Below are six examples of unique email headers associated with these recent campaigns:



- From: **telstraemailbill_noreply8@online.telstra.com**
- From: **AccountsPayable@Norfolk.gov.uk**
- From: **scanner@"yourdomain"**
- From: **someone@bausch.com**
- From: **jpie.kibungu@(various state agency domain)**
- From: **mike@xencourier.co.uk**

ISIS: Limited Cyber Capability, Strong Intent, Unpredictable

The NJCCIC is not aware of any specific, credible ISIS-related cyber threats to NJ, though we continue to work with Federal and State partners to assess the terrorist group's capabilities and targeting intent. The NJCCIC assesses with low confidence that ISIS' core cyber capabilities remain low and limited to activities such as socially engineered account compromises, doxing, and website defacements. However, more capable international hacking groups have and are likely to continue conducting more advanced operations on behalf of or in support of ISIS, exploiting targets of opportunity with disruptive tactics such as distributed denial of service (DDoS) attacks, as well as the theft and disclosure of sensitive data. In October, a media report indicated that ISIS was attempting intrusions on the US energy sector, however, these attempts were unsuccessful, affirming the current assessment of the group's low capability. The

NJCCIC is closely monitoring the cyber threat posed by terrorist groups and will provide more information in forthcoming threat analysis reports.

Threat Analysis

XSS - Many Websites Remain Vulnerable to Common Web Exploit

The NJCCIC assesses with moderate confidence that many websites remain at high risk of cross-site scripting (XSS), one of the most commonly exploited web application security vulnerabilities. XSS is a code injection tactic–similar to SQL injection–in which a hacker inputs malicious code into a legitimate web application or website that is then executed in a user's web browser, often to compromise user credentials or take control of the user's session. XSS exploits weaknesses in common scripting languages present in internet browsers, such as JavaScript, HTML, and Flash. The InfoSec Institute, provider of information security training, classifies XSS as one of the most dangerous website vulnerabilities and security researchers have identified the flaw in many high-traffic websites, often disclosed on a website dedicated to XSS vulnerabilities. For more information, please read the full product.

NJCCIC Announcements

With the start of the holiday shopping season approaching, the NJCCIC will be providing our members with information and resources to protect you and your families' personal and financial data, whether its shopping online or in-store. Follow the NJCCIC on Twitter @NJCybersecurity and Facebook next week for a series of daily tips and best practices.

Breach Notification

Starwood Hotels Announces Data Breach

Today, Starwood announced a point-of-sale data breach that compromised payment card data from customer transactions at properties across North America, including numerous Sheraton, W, and Westin hotels. The locations and potential dates of exposure for each affected Starwood property are listed here. The total number of victims is unknown at this time.

Tip of the Week

"Online Shopping Tips"

- Conduct research: When using a new website for purchases, read reviews and see if other consumers have had a positive or negative experience with the site.

- When in doubt, throw it out: Links in emails, posts and texts are often the ways cybercriminals try to steal your information or infect your devices.
- Personal information is like money: Value it and protect it: When making a purchase online, be alert to the kinds of information being collected to complete the transaction. Make sure you think it
  is necessary for the vendor to request that information. Remember, you only need to fill out required fields at checkout.
- Use safe payment methods: Credit cards are generally the safest option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered.
- Don't be disappointed: Read return and other policies so you know what to expect if the purchase doesn't go as planned
- Protect your $$: When shopping, check to be sure the site is security enabled. Look for web addresses with https:// indicating extra measures to help secure your information.

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/.

Share this email:

Manage your preferences | **Opt out** using **TrueRemove**™
Got this as a forward? **Sign up** to receive our future emails.
View this email **online**.

communications@njohsp.gov
Trenton, NJ | 08625 US

This email was sent to mvance@cyber.nj.gov.
To continue receiving our emails, add us to your address book.

powered by emma