NJCCIC
NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | November 25, 2015

Alert: Password Recovery Scam Attempts to Bypass Two-Factor Authentication

The NJCCIC received an incident report regarding a new tactic attackers are using to gain unauthorized access to online accounts with two-factor authentication (2FA) enabled, such as email or cloud storage services. This method works by tricking unassuming victims into believing they received a legitimate text message from the targeted account. First, the attacker obtains the victim's email address and mobile number. Then, he or she makes use of the password recovery feature offered by the target account which, most often, sends a verification code to the victim's mobile device associated with the account. Once the code is sent to the victim's mobile phone, the attacker sends the victim a text message spoofed to look like it has originated from the target account. The attacker's text asks the victim to reply with the legitimate verification code. If the victim responds with the code, the attacker can then access the victim's account and quickly changes the password and other account settings to prevent the victim from regaining control of the account. For a video demonstration of this tactic, see here.

Recommendations:

- Enable 2FA on all online accounts that offer it as a security setting.
- Be suspicious of any unsolicited text messages containing or asking for verification codes.
- If available, enable security settings to monitor what devices and locations are accessing your account and set up alerts for unusual activity.
- Change your passwords immediately if you suspect any unauthorized access.
- Remember, 2FA verification notifications will never ask the user to respond with the code.

Threat Analysis

Extortion: Profit-Motivated Cyber Tactics On the Rise

NJ Cyberlog

Cyber Tips for the Holiday Shopping Season

The NJCCIC assesses with high confidence that profit-motivated cyber extortion schemes such as ransomware and ransom-demanding distributed denial of service (DDoS) threats are likely to persist as effective and lucrative criminal tactics into 2016, with cumulative US losses likely to continue climbing into the hundreds of millions of dollars. These schemes have steadily grown in frequency and sophistication over the last year, with numerous new variants and capabilities emerging, such as the fourth iteration of the damaging CryptoWall ransomware family and a new ransomware strain targeting Linux-based operating systems often found on web servers. In addition to file-encrypting malware, other tactics are being employed to extort victims, such as blackmail and threats of disruptive DDoS attacks.

Ahead of Black Friday, Cyber Monday, and the rest of the holiday shopping season, the NJCCIC compiled the following cyber tips and best practices to help our fellow New Jerseyans stay safe by taking proactive steps to protect personal and financial information, and reduce the risk of falling victim to cybercrime. The holiday shopping season is an attractive time for criminals and fraudsters to take advantage of unsuspecting victims. The National Retail Federation expects spending this holiday season to reach upwards of $630 billion, with $105 billion of online spending. Find out what you can do to improve your information security and stay safe online this holiday season.

Breach Notification

Hilton Worldwide Point-of-Sale Breach

On Tuesday, Hilton Worldwide confirmed a previously reported, but unconfirmed, point-of-sale data breach that compromised customer transactions over a seventeen-week period, from November 18 to December 5, 2014 and April 21 to July 27, 2015, at an undisclosed number of Hilton hotel properties. The company has not disclosed the number of potential victims, or the specific properties involved in the breach. Customers can visit hiltonworldwide.com for more details, including how to receive one year of complimentary credit monitoring.

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/.