NJCCIC
NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | February 5, 2016

Update: Landry's Breach Impacts Tri-State Locations

On January 29, Landry's, Inc. provided an update on an investigation that began in December, confirming many of their nationwide restaurant locations were involved in a point-of-sale (PoS) malware breach. Payment card information was stolen from PoS terminals between May 4, 2014 and December 3, 2015.

Affected locations in New Jersey include **Big Fish Seafood Bistro** in Princeton; **Golden Nugget**, parking, banquets, spa and salon in Atlantic City; **McCormick & Schmick's** in Bridgewater and Cherry Hill (which has since closed); **Oceanaire Seafood Room** in Hackensack; **Rainforest Cafe** in Atlantic City; **Vic & Anthony's Golden Nugget** in Atlantic City.

Customers who made purchases at any of the affected Landry's locations during the specified timeframes should remain vigilant in reviewing their accounts for fraudulent activity. Any unauthorized charges should be reported immediately to the payment card provider. As a precautionary measure, victims may request a new payment card from their provider. Landry's customers with questions can call (877) 238-2151.

NJCCIC Comment: *The NJCCIC assesses the hospitality and restaurant industries remain at high risk of PoS breaches, due in-part to the slow adoption of the more secure EMV payment card technology, also known as Chip-and-PIN.* In 2015, several of the nation's largest hotel-operators experienced PoS breaches, including Hilton, Hyatt, Mandarin Oriental, Starwood, and the Trump Collection. Additionally, the vendors of PoS terminals used in restaurants throughout the country have been targeted over the last two years, including Harbortouch, NEXTEP, Signature Systems, and Advanced Restaurant Management Applications. For more information, including mitigation strategies, read our threat analysis titled "PoS Malware: Continued Threat to Businesses and Consumers".

Breach Notification

Latest Cyber Alerts

University of Central Florida

On Thursday, the University of Central Florida announced an intrusion into their network that exposed the Social Security numbers of approximately 63,000 current and former students, staff and faculty members. The University is offering victims one year of free credit monitoring and identity-protection services.

TaxSlayer

On January 13, tax preparation software publisher, TaxSlayer, identified that an unauthorized party may have accessed some of its customers' data through a third party vendor between October 10, 2015 and December 21, 2015. TaxSlayer has sent letters to notify the approximately 8,800 affected customers and is offering 12 months of credit monitoring.

Neiman Marcus

On January 29, Neiman Marcus notified potentially affected online customers of a breach that compromised approximately 5,200 accounts. Neiman Marcus' fraud team detected unauthorized purchases on at least 70 accounts and customer information was likely obtained. Customers are advised to change their account passwords and be on the look out for phishing emails.

A Vulnerability in GNU C Library Could Allow for Arbitrary Code Execution

Multiple Vulnerabilities in Google Android Could Allow for Remote Code Execution

Multiple Vulnerabilities in WordPress Content Management System Could Allow for Information Disclosure

Cyber In The News

The U.S. Just Struck A Crucial Deal With Europe On Data Privacy
via The Huffington Post

DHS to Start Sharing Cybersecurity Threat Indicators With Industry
via The Wall Street Journal

Passwords, Email Addresses, Were Most Stolen Data in 2015
via Dark Reading

Critical' Israwl power grid attack was just boring ransomware
via The Register

Oracle is planning to kill an attacker's favorite: the Java browser plug-in
via CSO Online

How to Avoid the Common Pitfalls While Browsing the Web
via Recorded Future

Tip of the Week

"Avoid Tax Season Scams"

IRS Commissioner warns of common tactics used by scammers:

- Call to demand immediate payment.
- Require a specific payment method, i.e. prepaid debit card.
- Ask for credit or debit card numbers over the phone.
- Threaten to have you arrested for not paying.

More information of current tax scams and tactics.

Impact: 5,000 victims cheated out of $26.5 million since 2013

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