NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Payment Cards: Threat Remains High Despite Chip Card Transition

June 17, 2016

TLP: **WHITE | *The NJCCIC assesses with high confidence that financially motivated cyber threats targeting American consumers' payment cards will remain high until the vast majority of point-of-sale (PoS) terminals in the United States are updated and certified to complete Europay, MasterCard, and Visa (EMV) transactions, as well as mobile payments.*** We further assess that cybercriminals will aggressively target the retail, hospitality, restaurant, and entertainment venue industries in the near term, as opportunities to exploit the insecure magnetic stripe diminish.

"Swipe-and-sign" transactions will continue to pose a high risk of compromise and consumers who frequently use debit cards for purchases, or to conduct ATM cash withdrawals, are at a higher risk of financial loss if victimized by PoS malware or skimming devices. When debit card account information is stolen, criminals can make large purchases or withdrawal the full balance of the associated checking account with no guarantee the victim will recover all of their funds.

- In the wake of the Target and Home Depot breaches of 2013 and 2014 respectively, PoS breaches resulting from malware infections continue to be a regular occurrence in the United States. The nationwide food chain Wendy's recently acknowledged an ongoing investigation into a widespread PoS malware infection at locations throughout the country. According to their latest press release, the number of locations impacted by the breach is "considerably higher" than originally reported in May. In March, investigative journalist Brian Krebs reported that credit unions were observing large increases in debit card fraud resulting from the Wendy's breach. Over the last two years, Krebs has detailed numerous PoS breaches involving hotel chains, restaurants, grocery stores, parking services, and PoS device vendors.
- While some nationwide retailers and local small business vendors have updated PoS terminals to accept EMV payments, and many Americans have received new payment cards with the embedded chip that enables a more secure transaction, the United States has not fully adopted the combined "chip-and-PIN" standard. Therefore, many "card-present" transactions with chip-enabled cards continue to be verified using a customer's signature as opposed to a personal identification number (PIN), leaving consumers and retailers vulnerable to fraud. Two US-based retailers, Home Depot and Walmart, are separately suing two of the Nation's largest credit card companies, alleging the corporations are intentionally preventing retailers from requiring PINs instead of customer signatures.
- Skimming devices also pose a significant financial threat to Americans, both stateside and while traveling aboard. According to an alert published by the Fair Isaac Corporation in April, 2015 saw the highest ever number of ATM compromises in the United States, a 546 percent increase from 2014. Notably, ATMs and gas station pumps—the two most likely locations for skimming devices—were largely exempt from the October 2015 EMV liability shift and deadline to accept chip cards, with an extension to implement EMV-capable terminals by October 2017. Thus, until all US cardholders are issued EMV-enabled credit and debit cards, and all ATMs and PoS systems are modified to no longer read the magnetic stripe, the threats posed by malware and skimming devices will persist.

Recommendations for Businesses

The NJCCIC encourages businesses to take a proactive approach to preventing PoS breaches by implementing a comprehensive cybersecurity strategy, including changes to network architecture, policies and procedures, and the regular training of employees to mitigate the risk of spear-phishing and other social engineering tactics used to gain initial access to a business network. For specific recommendations, and detailed information on current PoS malware variants, please visit the NJCCIC's PoS Malware Threat Profile.

- Additional technical recommendations can be found in a recent whitepaper published by SANS, titled "Beyond the Point of Sale: Six Steps to Stronger Retail Security".

Traffic Light Protocol: **WHITE** information may be distributed without restriction.