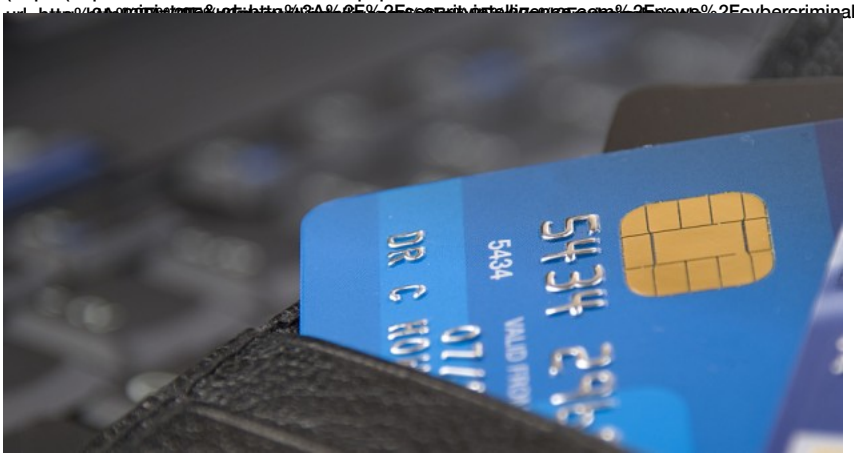
NEWS April 11, 2018 @ 12:21 PM

Cybercriminals Use Old-School Tactics to Exploit Credit Card Chip Security

By Douglas Bonderud (https://securityintelligence.com/author/douglas-bonderud/)



Thinkstock (http://www.thinkstockphotos.com/image/stock-photo-close-up-photo-of-a-blue-credit-card-emerging/144347794/popup?sq=credit card chip/f=CPHX/p=3/s=DynamicRank)

Credit card fraud is on the rise. As noted by an October 2016 issue of The Nilson Report (https://nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf), global losses topped $21 billion in 2015 and show no signs of slowing, even with the adoption of supposedly secure Europay, MasterCard and Visa (EMV) chip-and-PIN cards.

Part of the problem comes from increased fraud activity across e-commerce channels, which often allow card-not-present (CNP) purchases that circumvent chip-and-PIN technology (https://securityintelligence.com/chip-and-pin-fraud-the-new-face-of-credit-crime/). However, authorities recently uncovered a low-tech scam to compromise credit card chip security that primarily targets large enterprises.

Fraudsters Intercept Chip-and-PIN Cards

According to Krebs on Security (https://krebsonsecurity.com/2018/04/secret-service-warns-of-chip-card-scheme/), the U.S. Secret Service recently reported that enterprising cybercriminals are intercepting corporate chip-and-PIN cards sent directly by issuing financial institutions. These cards often access business accounts for travel or work-related purchases, meaning there's no shortage of funds available. Attackers, recognizing the futility of beating credit card chip security, instead opt to bypass it altogether.

First, they intercept the bulk cards and use a heat gun to pry off new chips. Old chips are then attached to the cards before they're sent off to their destination. After companies activate their new cards, they discover that the cards don't work because the chips aren't valid. The newly chipped criminal cards, however, work just fine, giving attackers full access to corporate bank accounts.

Instead of trying to beat chip-and-PIN security at its own game, attackers leverage secure chips themselves as an effective means to compromise. According to PC Magazine (https://www.pcmag.com/news/360270/criminals-are-replacing-chips-on-new-debit-cards), the best course of action for concerned companies may be to pay banks for tracked, secure shipping methods to ensure that cards aren't compromised en route.

Emerging Trends in Credit Card Chip Security

TRENDING NEWS

The IoT and Cybersecurity: Governments Step Up as Industries Struggle (https://securityintelligence.com/news/the-iot-and-cybersecurity-governments-step-up-as-industries-struggle/)

Read More (https://securityintelligence.com/news/the-iot-and-cybersecurity-governments-step-up-as-industries-struggle/)

The New State of Cybersecurity: Bursts, Worms and Mobile Threats (https://securityintelligence.com/news/the-new-state-of-cybersecurity-bursts-worms-and-mobile-threats/)

Read More (https://securityintelligence.com/news/the-new-state-of-cybersecurity-bursts-worms-and-mobile-threats/)

Cybercrime-as-a-Service Offerings Include DDoS Attacks Starting at $10, Report Reveals (https://securityintelligence.com/news/cybercrime-as-a-service-offerings-include-ddos-attacks-starting-at-10-report-reveals/)

Read More (https://securityintelligence.com/news/cybercrime-as-a-service-offerings-include-ddos-attacks-starting-at-10-report-reveals/)

(https://securityintelligence.com/events/rsa-2018/)

(https://securityintelligence.com/2018-ibm-x-force-report-shellshock-fades-gozi-rises-and-

While chip-and-PIN cards have dramatically reduced the incidence of in-store fraud, according to Visa (https://usa.visa.com/visa-everywhere/security/visa-chip-card-stats.html), new tactics such as mail interception show that criminals aren't giving up — they're just developing new methods (https://securityintelligence.com/chip-and-pin-fraud-the-new-face-of-credit-crime/). As noted by Retail TouchPoints (https://www.retailtouchpoints.com/features/executive-viewpoints/three-e-commerce-fraud-challenges-to-beat-in-2018), this means an uptick in both new attack vectors and old-school methods to circumvent defenses.

On the sophisticated side of the equation, cybercriminals are now choosing collaboration over lone action, allowing them to infiltrate systems and hide out for months before making their move, Forbes (http://fortune.com/2017/09/21/equifax-data-breach-hacked-march/) reported. By targeting vulnerable devices and internet-facing services, actors can sidestep the need for chip-and-PIN cards and go straight to the source of payment data. There's also a significant uptick in mail order and telephone order (MOTO) fraud in which attackers phone in orders to call centers that don't have protections against card-not-present fraud, according to Retail TouchPoints .

Credit card chip security has pushed fraud out of stores and into e-commerce. As retail websites improve protection, attackers are leveraging physical interception and digital subterfuge in an effort to both bypass chip-and-PIN defenses and leverage this technology for their own gain.

Tags: Credit Card Fraud (https://securityintelligence.com/tag/credit-card-fraud/) | Credit Card Theft (https://securityintelligence.com/tag/credit-card-theft/) | E-commerce (https://securityintelligence.com/tag/e-commerce/) | EMV (https://securityintelligence.com/tag/emv/) | Fraud (https://securityintelligence.com/tag/fraud/) | Fraud Protection (https://securityintelligence.com/tag/fraud-protection/) | Payment Card Industry (PCI) (https://securityintelligence.com/tag/payment-card-industry-pci/) | Retail (https://securityintelligence.com/tag/retail/) | Retail Security (https://securityintelligence.com/tag/retail-security/)

Share this Article:

RECOMMENDED ARTICLES

(https://securityintelligence.com/news/the-iot-and-cybersecurity-governments-step-up-as-industries-struggle/)

March 22, 2018

The IoT and Cybersecurity: Governments Step Up as Industries Struggle (https://securityintelligence.com/news/the-iot-and-cybersecurity-governments-step-up-as-industries-struggle/)

By Douglas Bonderud (https://securityintelligence.com/author/douglas-bonderud/)

(https://securityintelligence.com/news/the-new-state-of-cybersecurity-bursts-worms-and-mobile-threats/)

March 19, 2018

The New State of Cybersecurity: Bursts, Worms and Mobile Threats (https://securityintelligence.com/news/the-new-state-of-cybersecurity-bursts-worms-and-mobile-threats/)

By Douglas Bonderud (https://securityintelligence.com/author/douglas-bonderud/)

(https://securityintelligence.com/news/cybercrime-as-a-service-offerings-include-ddos-attacks-starting-at-10-report-reveals/)

March 26, 2018

Cybercrime-as-a-Service Offerings Include DDoS Attacks Starting at $10, Report Reveals (https://securityintelligence.com/news/cybercrime-as-a-service-offerings-include-ddos-attacks-starting-at-10-report-reveals/)

By Shane Schick (https://securityintelligence.com/author/shane-schick/)

Douglas Bonderud (https://securityintelligence.com/author/douglas-bonderud/)

Freelance Writer

A freelance writer for three years, Doug Bonderud is a Western Canadian with expertise in the fields of technology and innovation. In addition to working for the IBM Midsize Insider, The Content Standard and Proteomics programs for Skyword, Doug also writes for companies like Ephricon Web Marketing and sites such as MSDynamicsWorld. Clients are impressed with not only his command of language but the minimal need for editing necessary in his pieces. His ability to create readable, relatable articles from diverse Web content is second to none. He has also written a weekly column for TORWars, a videogaming website; posts about invention and design for InventorSpot.com and general knowledge articles for WiseGeek. From 2010-2012, Doug did copywriting for eCopywriters.com. Doug is currently a municipal police officer, on track to become a fantasy/sci-fi author.

SEE ALL POSTS →

(/become-a-contributor/)

Become a Contributor

APPLY (/BECOME-A-CONTRIBUTOR/)

(https://securityintelligence.com)

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of IBM.

NEWS (HTTPS://SECURITYINTELLIGENCE.COM/NEWS/)

TOPICS (HTTPS://SECURITYINTELLIGENCE.COM/CATEGORY/TOPICS/)

INDUSTRIES (HTTPS://SECURITYINTELLIGENCE.COM/CATEGORY/INDUSTRIES/)

X-FORCE RESEARCH (HTTPS://SECURITYINTELLIGENCE.COM/CATEGORY/X-FORCE/)

MEDIA (HTTPS://SECURITYINTELLIGENCE.COM/MEDIA/)

EVENTS & WEBINARS (HTTPS://SECURITYINTELLIGENCE.COM/EVENTS/)

ABOUT US (HTTPS://SECURITYINTELLIGENCE.COM/ABOUT-US/)

CONTRIBUTORS (/CONTRIBUTORS)

BECOME A CONTRIBUTOR (HTTPS://SECURITYINTELLIGENCE.COM/BECOME-A-CONTRIBUTOR/)

(http://feeds.feedburner.com/Se

(http://www.twitter.com/ibmsecu

(http://facebook.com/ibmsecurit

(https://www.youtube.com/c/IBI

(http://www.linkedin.com/security)

(http://slideshare.net/ibmsecurit

(https://www.quora.com/IBM-Security/)

(http://ibm.com/security?ce=ISM0484&ct=SWG&cmp=IBMSo

© 2018 IBM (http://www.ibm.com?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) | Contact (https://www.ibm.com/contact/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) | Privacy (https://www.ibm.com/privacy/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) | Terms Of Use (https://www.ibm.com/legal/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) | Accessibility (https://www.ibm.com/accessibility/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US)