2012 Payment Card Threat Report

The second annual study of unencrypted payment card storage

SecurityMETRICS®

Automated Attacks and Card Data Handling

In 2011, data breaches increased 42% and as such, last year was reported one of the greatest successes of all time for criminals.[1]

What propagates the widespread reach and effectiveness of cyber criminals? The availability of automated hacking tools. In early 2012, a single teenager hacked nearly 260 websites in a three-month period with automated tools commonly found in crimeware toolkits[2]. Crimeware toolkits are pre-crafted hacking software that expose vulnerabilities on business networks and are readily available to the masses online. Today, at least 61% of online attacks begin with or utilize automated crimeware toolkits[3].

In addition, standalone tools on the black market used to maliciously scan, infect, and pull sensitive data from systems are dropping in price. Password crackers, software used to decipher passwords, are downloadable for free. Most malware now sells in the mere hundred-dollar range compared to thousands of dollars in the past, and can be custom ordered for specific targets[4].

What are the effects of automated, cheap, and easily available hacking tools? The answer is worldwide credit card fraud that amounts to $5.55 billion[5].

Criminals are heavily armed with the necessary tools to access business networks and are successfully stealing sensitive data.

This is the second annual study that demonstrates how the majority of merchants make cybercriminals' jobs easier. As cybercriminals are heavily armed with the necessary tools to conduct cyber attacks, many businesses continue to leave payment card data on their network; unencrypted and ready for the taking.

Not storing unencrypted payment card data significantly increases the difficulty of stealing payment card data. The overall purpose of this study is to decrease cybercriminal success by motivating businesses to locate, delete, and stop storage of unencrypted payment card data.

Types of Payment Card Data

> "I had no idea I was storing credit cards."

This is a common response made by businesses to SecurityMetrics Payment Card Industry Forensic Investigators (PFI) after discovering their business was targeted and breached by criminals. Many businesses do not realize payment card data may be stored behind the scenes of their computer systems – leaving data unprotected, and readily available for criminals to confiscate.

Not only are businesses burdened with protecting cardholder data, but must pay compromise investigation and recovery costs if data is stolen from systems.

Simply put, the more data is stolen, the greater the business liability to fines and penalties.

Primary account numbers (PAN) from all major card brands (Visa, MasterCard, American Express, Discover, and JCB) are among the most common type of data found on business networks. Though it is against Payment Card Industry (PCI) security requirements, some businesses continue to retain encrypted and unencrypted magnetic stripe track data, which acts as the card's blueprint. Possessing track data, which includes the PAN, cardholder information, expiration date, and three-digit service code, makes for effortless payment card duplication.

securityMETRICS®

Black Market Sales

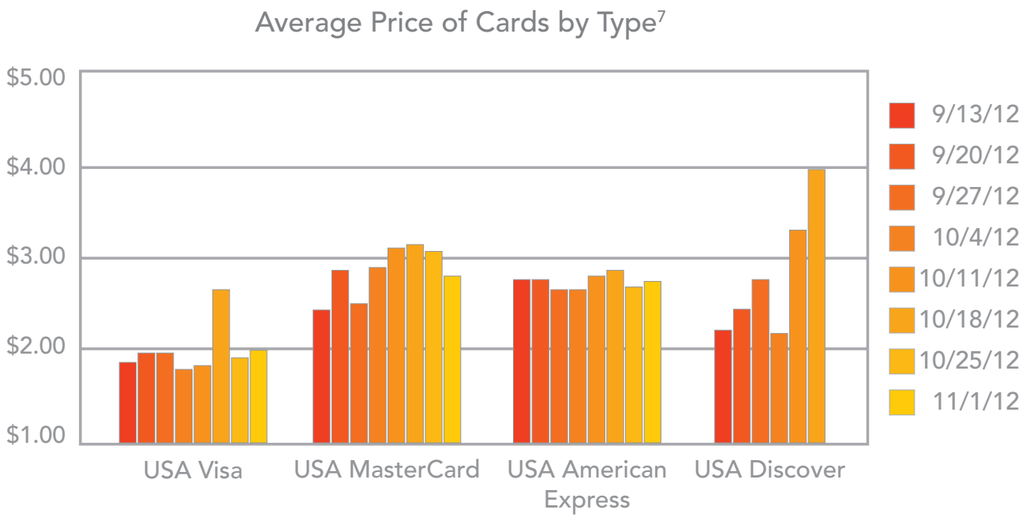
Depending on card type, card origination, and the laws of supply and demand, harvested payment card details can be purchased for an average of $2 per card.

The sales process begins through illegal online "carding" forums where buyers must undergo a series of screenings to participate. For example, many forums require participants to be referred by at least two current members to join. The forums act as a connection point between buyers and sellers where actual transactions take place elsewhere. Because of the illegal nature of carding sites, they are constantly closing and reopening under different web domains.

Once a trusted relationship is made, and consumer confidence is established, purchasing card data is simple. U.S. Attorney Neil H. MacBride recently said:

> "Countless lives are thrown into financial turmoil because of these websites, with a few simple clicks, thousands of stolen credit card numbers can be bought or sold to fraudsters anywhere in the world. Today's seizures are part of an ongoing campaign to disrupt this online market regardless of where it operates."[6]

Even though seizures are taking place, carding forums are still thriving. This is why taking multiple measures to protect payment card data is so important, including discovering if payment card data is leaking into a business network.



Leaking Payment Card Data

Unencrypted payment card data may get saved, or leak on a business network from a variety of sources. Often, the extent of data leakage makes manual discovery of unencrypted payment card data nearly impossible. A manual search requires enough time and effort to search through all systems drive-by-drive and file-by-file. The process could take weeks or even months to complete, depending on the amount of available resources and business network size.

While conducting PCI DSS audits, SecurityMetrics Qualified Security Assessors (QSA) have identified the following as common locations of payment card data leaking into business networks.

- Accounting—book balancing, charge reversals, employee workstations
- Sales—shopping carts, email payments, recurring billing
- Marketing—purchase trend research
- Engineering—computer program test environments
- Customer Service—documented phone orders, refunds
- Administration—employee workstations

Unencrypted Payment Card Data Storage

Unencrypted payment card data storage is attractive to criminals because it requires little work to extract from systems. From Q1-Q3, SecurityMetrics studied over 2,700 first-time payment card data discovery scans to uncover the rate of card storage. The scans were conducted by merchants of all sizes using SecurityMetrics' card data discovery tool PANscan®.

Study results demonstrate there hasn't been a major change in the amounts of storage since last year.

Unencrypted payment card data storage continues to plague merchants.

Number of machines scanned.....2,754

Total Gigs scanned.....143,579

Total files scanned.....457,048,456

Total cards found.....315,639,164

Max cards found in single scan.....91,657,934

70.92%

of merchants store unencrypted payment card data on their business network.

10.53%

of merchants store magnetic stripe track data.

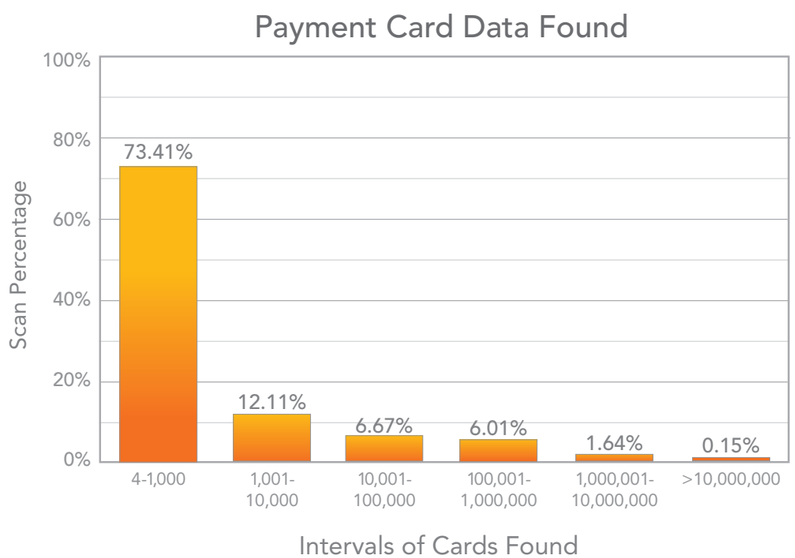
Of the 2,754 conducted,

315,639,164

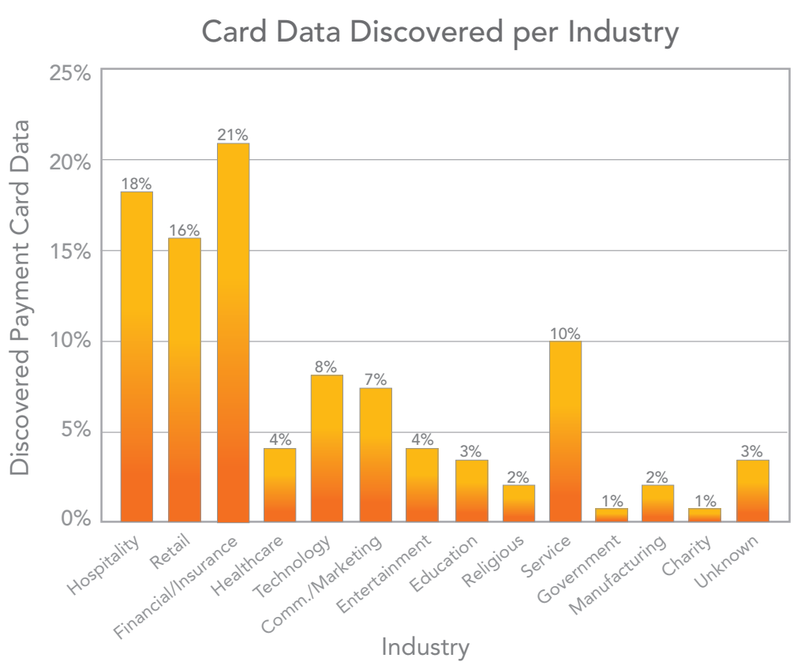
total payment cards were identified on business systems.

Storage of unencrypted PANs remained alarmingly high, only decreasing

.24%.



Similar to 2011 data, the overwhelming majority (73.41%) of payment card data identified by PANscan came from scans resulting in less than 1,000 discovered payment cards.



The three most impacted industries are financial, hospitality, and retail, accounting for 55% of the total unencrypted payment card data storage. Interestingly, these industries are the three most targeted by cybercriminals.[8]

securityMETRICS®

Successful Prevention

Successful prevention of unencrypted payment card data storage requires time and dedication, but it's worth it. The following section contains some things businesses can do to make the process a success.

Map pathways

Businesses must map all pathways of payment card data on a network. This ensures the flows of payment card data inside a network are known, so weak links in the chain can be removed. The map should begin with the obvious places first, e.g., payment servers, e-commerce servers, and drives that may contain payment transaction files.

Employ a card data discovery tool

Discovery tools increase the speed and accuracy of a search. Most tools are relatively inexpensive and dramatically save time.

When a business searches for a card data discovery tool, it should consider the following:

Price—Many tools are available for less than $100 per licensed machine, and some are free. It's good to keep in mind when purchasing a card data discovery tool, a business is really purchasing convenience, speed, and accuracy.

Processing power—Some scanning tools may require significant quantities of computer processing power and memory. This may affect a business' ability to conduct other system tasks simultaneously.

Accuracy—Many tests produce a large number of false positives. A false positive occurs when a scan concludes that a file contains card data, but in reality it does not. Most vendors of card data discovery tools manage false positives differently. To ensure the tool in consideration provides a simple solution for false-positive management, a business must inquire the vendor.

Create policies

To successfully remove unencrypted payment card data from systems, businesses must conduct searches on a regular basis. To ensure a regular or ongoing search for sensitive data, businesses must create a company policy surrounding card data discovery that details employee roles and procedures, when and where a search should be conducted, and the process for secure removal of the data.

Securely delete files

When a file is deleted without the use of a secure delete tool, the reference to conveniently access the file is removed, but the file remains on a system. Businesses must ensure sensitive payment card data is properly removed from a system through the use of a secure delete tool.

Don't Be Part of the 70%

Criminals need only invest a few hundred dollars in automated crimeware toolkits to initiate a barrage of attacks on businesses around the world. Unfortunately, they can count on 70% of all merchants to store unencrypted payment card data. By liberating systems of unencrypted payment cards, businesses can contribute to the overall decrease of cybercriminal success. After all, criminals cannot steal unencrypted payment card data if it's not on a system.

This study indicates that the majority of businesses leave low-hanging-fruit available for criminals, making theft much easier. Unless drastic measures are taken to delete and prevent unencrypted payment card data storage, criminals will continue to pillage the unsuspecting business.

Though the majority of businesses don't store large amounts of payment card data, automated attacks allow cybercriminals to conduct multiple simultaneous attacks, resulting in aggregated success. To avoid increased liability to fines and penalties, businesses must discover card data on business systems, securely delete it, patch sources of storage, and continue to check for unencrypted payment card data on a regular basis.

Sources:

1. Ponemon Institute, 2012 Cost of Cyber Crime Study: United States, October, 2012, Web: October 31, 2012, PDF
2. Mathew J. Schwartz, "Malware Toolkits Generate Majority Of Online Attacks", Informationweek, January, 2011, Web: November 5, 2012
3. Mathew J. Schwartz, "Malware Toolkits Generate Majority Of Online Attacks", Informationweek, January, 2011, Web: November 5, 2012
4. RSA, 2012 Cybercrime Trends Report: The Current State of Cybercrime and What to Expect in 2012, February 2012, Web: November 3, 2012, PDF
5. Consumer Sentinel Network and U.S. Department of Justice http://www.statisticbrain.com/credit-card-fraud-statistics/
6. Department of Justice: Office of Public Affairs, Federal Courts Order Seizure of 36 Website Domains Involved in Selling Stolen Credit Card Numbers, April 26, 2012, Web: Oct 31, 2012
7. CloudeyeZ, "Undergound Activity Index", Average price of cards by type, November, 2012, Web: November 8, 2012
8. Verizon, 2012 Data Breach Investigations Report, October, 2012, Web: November 4, 2012, PDF

About SecurityMetrics

SecurityMetrics is a global leader in merchant data security and compliance for all business sizes and merchant levels, and has helped over 1 million organizations manage PCI DSS compliance and/or secure their network infrastructure, data communication, and other information assets. As an Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Payment Application Qualified Security Assessor (PA QSA), Penetration Tester, and Payment Card Industry Forensic Investigator (PFI), SecurityMetrics has the tools available to help businesses achieve lasting security and validate accurate PCI compliance.

US Headquarters:
1275 West 1600 North
Orem, UT 84057
801.705.5665

UK Headquarters:
Victory House
400 Pavillion Drive
Northampton Business Park
Northampton NN4 7PA
+ 44 (0) 207 993 8030

productinfo@securitymetrics.com
www.securitymetrics.com