



May 19, 2015

AGA Utah Chapter 2015 Spring Conference

**PCI'S CHANGING ENVIRONMENT –
“WHAT YOU NEED TO KNOW & WHY
YOU NEED TO KNOW IT.”**

Kevin R Perry – PCI ISA, PCIP
kperry@utah.gov

**How in the world did we get here and WHY
is Securing Credit Card Data so Important?**



Home > Malware



Boston Liquor Store Hit With Point-of-Sale Malware

By Fahmida Y. Rashid on March 27, 2013

 Share 3
  0
  Tweet 34
  Recommend 9
  RSS

A Boston-based merchant warned customers this week that a “sophisticated malware attack” had compromised some customers' credit and debit card information. An investigation was underway and more details are expected later this week.

Blanchard's Liquors of Allston discovered last Friday that its point-of-sale (POS) systems had been infected with malware and some customer credit and debit card information may have been compromised, according to a statement on the store's Website. The company immediately took down its primary credit card terminals, removed the infection, and brought the system back online on Saturday.

Affected customers used their credit and debit cards at Blanchard's, whose storefront is located just west of Boston University. It's not known at this time how the POS system was infected, or which malware was used.

SecurityWeek reported this week on [vSkimmer](#), a new variant of the Dexter malware and [Dump Memory Grabber](#), two malware families specifically targeting POS systems to harvest user payment card details.



Exclusive: New Malware Targeting POS Systems, ATMs Hits Major US Banks

By Fahmida Y. Rashid on March 27, 2013

 Share 124
  34
  Tweet 206
  Recommend 146
  RSS

Attackers Exploited Vulnerabilities in ATM Networks Connecting to Bank VPNs and GSM/GPRS Networks, Malware Infected ATMs and POS Systems to Steal Card Data.

A new malware targeting point-of-sale (POS) systems and ATMs has stolen payment card information from several US banks, researchers say. The author behind the malware appears to have links to a Russian cyber-crime gang.

Called “Dump Memory Grabber”, the malware scans the memory of point-of-sale systems and ATMs looking for credit card data, researchers from Russia-based security company [Group-IB](#) told *SecurityWeek*. The researchers believe the malware has already been used to steal data from credit and debit cards issued by major US banks, including Chase, Capital One, Citibank, and Union Bank of California.



SecurityWeek viewed a video allegedly posted by the author of Dump Memory Grabber on an underground forum which listed some of the stolen card numbers. It appears some customers with Nordstrom-branded credit cards may have also been compromised.

“We have found one of the C&C servers for the following POS malware, but in fact hundreds of

Malware on point-of-sale terminals behind Target hack, at least three other well-known US retailers hit using similar methods

By Jose Vilches

On January 13, 2014, 10:30 AM

13

Like 48

+1 8

Tweet 30



Luxury Retailer Neiman Marcus Admits To Breach In Customer Credit Card Information

January 12, 2014 3:18 PM

Like 14

Tweet 13

Share

3

View Comments



Michaels discloses possible customer data breach; Secret Service investigating



Reuters, JAN 26/No-Data-Available, JAN 26/Reuters - Michaels said that has not yet confirmed a breach, but wanted to warn customers in light of other cyber attacks on retailers such as Target and Neiman Marcus.

10 Banks: Credit Card Breach at P.F. Chang's

JUN 14



Nationwide chain **P.F. Chang's China Bistro** said today that it is investigating claims of a data breach involving credit and debit card data reportedly stolen from restaurant locations nationwide.

On June 9, thousands of newly-stolen credit and debit cards went up for sale on [rescator\[dot\]so](#), an underground store best known for selling **tens of millions of cards stolen in the Target breach**. Several banks contacted by KrebsOnSecurity said they acquired from this new batch multiple cards that were previously issued to customers, and found that all had been used at P.F. Chang's locations between the beginning of March 2014 and May 19, 2014.

Contacted about the banks' claims, the Scottsdale, Arizona-based restaurant chain said it has not yet been able to confirm a card breach, but that the company "has been in communications with law enforcement authorities and banks to investigate the source."



Home Depot's credit cards may have been hacked



Elizabeth Weise, USATODAY 9:46 a.m. EDT September 3, 2014



(Photo: Home Depot)

10742 465 363 42
CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

SAN FRANCISCO — A massive batch of credit and debit card information that went on sale on a criminal Internet site Tuesday may be from Home Depot stores and could be linked to hackers responsible for breaches at Target and P.F. Chang's, security experts say.

The credit card information was offered for sale Tuesday on an underground site that traffics in stolen financial information, journalist Brian Krebs reported on his blog, Krebsonsecurity.com.

The breach could have begun in late April or early May of this year, Krebs reported.

If that is true, this incident could dwarf the [Target breach](#), in which 40 million credit and debit accounts were compromised over a three-week period.

"This latest batch of cards is for sale from the same underground store that sold cards from P.F. Chang's and Target," said Trey Ford, a security strategist at [Rapid7](#), a Boston-based computer security company.

NERC CIP O
COMPLIAN

www1.gotomeeting.com/

Free Webcast with Lela

Oct 23 Developing Y

Security Plan

The Cybercrime Economy

Albertson's stores hacked for credit card data

By Jose Pagliery @Jose_Pagliery August 15, 2014: 11:48 AM ET



PHOTO: ETHAN MILLER/GETTY IMAGES

Albertson's and Shop 'N Save became the latest companies to experience a data breach of its debit and credit card data.

NEW YORK (CNNMoney)

Hackers have broken into the credit and debit card payment networks at two of the nation's most popular supermarket store chains: Albertson's and SuperValu.

16 Breach at Goodwill Vendor Lasted 18 Months

SEP 14

C&K Systems Inc., a third-party payment vendor blamed for a credit and debit card breach at more than 330 **Goodwill** locations nationwide, disclosed this week that the intrusion lasted more than 18 months and has impacted at least two other organizations.

On July 21, 2014, this site **broke the news** that multiple banks were reporting indications that Goodwill Industries had suffered an apparent breach that led to the theft of customer credit and debit card data. Goodwill later **confirmed** that the breach impacted a portion of its stores, but blamed the incident on an unnamed "third-party vendor."



Last week, KrebsOnSecurity obtained **some internal talking points** apparently sent by Goodwill to prepare its member organizations to respond to any calls from the news media about the incident. Those talking points identified the breached third-party vendor as C&K Systems, a retail point-of-sale operator based in Murrells Inlet, S.C.

In response to inquiries from this reporter, C&K released a statement acknowledging that it was informed on July 30 by "an independent security analyst" that its "hosted managed services environment may have experienced unauthorized access." The company says it then hired an independent cyber investigative team and alerted law enforcement about the incident.

24 Jimmy John's Confirms Breach at 216 Stores

SEP 14



More than seven weeks after this publication **broke the news** of a possible credit card breach at nationwide sandwich chain **Jimmy John's**, the company now confirms that a break-in at one of its payment vendors jeopardized customer credit and debit card information at 216 stores.

On July 31, KrebsOnSecurity reported that multiple banks were seeing a pattern of fraud on cards that were all recently used at Jimmy John's locations around the country. That story noted that the company was working with authorities on an investigation, and that multiple Jimmy John's stores contacted by this author said they ran point-of-sale systems made by Newtown, Pa.-based **Signature Systems**.



In a statement issued today, Champaign, Ill. based Jimmy John's said customers' credit and debit card data was compromised after an intruder stole login credentials from the company's point-of-sale vendor and used these credentials to remotely access the point-of-sale systems at some corporate and franchised locations *between June 16, 2014 and Sept. 5, 2014*.

LIST: Dairy Queen says 395 stores hit by data breach

POSTED 6:54 AM, OCTOBER 10, 2014, BY [CNN WIRE](#), UPDATED AT 06:57AM, OCTOBER 10, 2014

[TWITTER](#) [FACEBOOK](#) [GOOGLE](#) [LINKEDIN](#) [PINTEREST](#) [EMAIL](#)

Dairy Queen is the latest company to get hit by a security breach saying that payment card data has been impacted at nearly 400 of its restaurants around the country.



The ice cream stand operator said malware called Backoff is to blame, and that it accessed systems through a "third-party vendor's compromised account credentials." The company also said the malware has been "contained."

The hacked systems contained customer names, payment card numbers and expiration dates, according to the company.

On Thursday, Dairy Queen published an online list of the 395 restaurants where payment card data was affected. Orange Julius locations were also affected. [FULL LIST HERE](#). The company has about 4,500 outlets.

10 Malware Based Credit Card Breach at Kmart

OCT 14



Sears Holding Co. late Friday said it recently discovered that point-of-sale registers at its **Kmart** stores were compromised by malicious software that stole customer credit and debit card information. The company says it has removed the malware from store registers and contained the breach, but that the investigation is ongoing.

"Yesterday our IT teams detected that our Kmart payment data systems had been breached," said **Chris Brathwaite**, spokesman for Sears. "They immediately launched a full investigation working with a leading IT security firm. Our investigation so far indicates that the breach started in early September."

According to those investigators, Brathwaite said, "our systems were infected with a form of malware that was currently undetectable by anti-malware systems. Our IT teams quickly removed that malware, however we do believe that debit and credit card numbers have been compromised."

Brathwaite stressed that the data stolen included only "track 2" data from customer credit and debit cards, and did not include customer names, email address, physical address, Social Security numbers, PINs or any other sensitive information.

20 Banks: Credit Card Breach at Staples Stores

OCT 14



Multiple banks say they have identified a pattern of credit and debit card fraud suggesting that several **Staples Inc.** office supply locations in the Northeastern United States are currently dealing with a data breach. Staples says it is investigating “a potential issue” and has contacted law enforcement.

According to more than a half-dozen sources at banks operating on the East Coast, it appears likely that fraudsters have succeeded in stealing customer card data from some subset of Staples locations, including seven Staples stores in Pennsylvania, at least three in New York City, and another in New Jersey.



Framingham, Mass.-based Staples has more than 1,800 stores nationwide, but so far the banks contacted by this reporter have traced a pattern of fraudulent transactions on a group of cards that had all previously been used at a small number of Staples locations in the Northeast.

The fraudulent charges occurred at other (non-Staples) businesses, such as supermarkets and other big-box retailers. This suggests that the cash registers in at least some Staples locations may have fallen victim to card-stealing malware that lets thieves create counterfeit copies of cards that customers swipe at compromised payment terminals.

Breaches Continue in 2015

- **Marriott Hotels**
 - 2nd time for White Lodging Services
- **Chick-fil-A (Suspected)**
 - April 27, 2015 case closed and no breach evidence found
- **Hard Rock Hotel – Restaurant and Gift Shop**
 - Malware went undetected for 7 months including exfiltration
- **Mandarin Oriental – The Hotel Group**
- **Sally Beauty – Just two weeks ago**
 - 2nd time since March 2014
- **?? Who's next??**

Officials warn 500 million financial records hacked

Erin Kelly, USA TODAY 8:10 p.m. EDT October 20, 2014



(Photo: David Goldman, AP)

f 8122 TWEET 1064 in 656 COMMENT 92 EMAIL MORE

WASHINGTON — Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building.

"We're in a day when a person can commit about 15,000 bank robberies sitting in their basement," said Robert Anderson, executive assistant director of the FBI's Criminal Cyber Response and Services Branch.

The U.S. financial sector is one of the most targeted in the world, FBI and Secret Service officials told business leaders at a cybersecurity event organized by the Financial Services Roundtable. The event came in the wake of mass hacking attacks against Target, Home Depot, JPMorgan Chase and other financial institutions.

"You're going to be hacked," Joseph Demarest, assistant director of the FBI's cyberdivision, told the business leaders. "Have a plan."

BEYOND PENALTIES AND FINES

"Forty percent of consumers change their relationship with a business affected by a security breach."

Linda Tucci, "PCI Standard Still Packs Little Punch," SearchCIO.com

PCI COMPLIANCE – TRENDS AND TIPS

PCI is not about securing sensitive data, it's
about eliminating data altogether.

John Kindervag, Forrester Analyst and former QSA



PCI OVERVIEW

- What is PCI DSS?
 - Payment Card Industry (PCI) Data Security Standard (DSS)
 - All member organisations that issue or acquire information from cards with the Visa, MasterCard, American Express and Discover logos are required to comply with a range of information security requirements.
- Where does it apply?
 - Applies to organisations where cardholder data is stored, processed, or transmitted.
- PCI DSS How does it work?
 - The PCI DSS standard sets common requirements for securing card information, and lays out a range of controls relating to auditing, scanning and assessment.



PCI OVERVIEW

- Why is it needed?
 - Encourage and enhance cardholder data security
 - Facilitates the broad adoption of consistent data security measures globally.
 - Prevent breaches of card data like “Example”
- Compliance
 - PCI Security Standards Council sets the requirements, but each card association implements and enforces the standard, fines/fees, and compliance levels and deadlines.
- Validation versus Compliance
 - Compliance: 24x7x365
 - Validation: Yearly task.

PCI OVERVIEW

- Do I really need to be PCI Compliant?
 - PCI is a contractual clause originating with the Card Brands
 - Not a legislative requirement.
 - Has Data Protection considerations
 - Card brand and/or acquiring bank could remove the facility to store/process/issue cards if not compliant.
 - Service Provider could lose merchants confidence.

THE TWELVE HIGH LEVEL REQUIREMENTS

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

CHANGE HIGHLIGHTS

Types of changes to the Standards are categorized as follows:

1. Clarification – Clarifies intent of requirement. Ensures that concise wording in the standard portrays the desired intent of requirements.
2. Additional Guidance – Explanation, definition, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
3. Evolving Requirement – Changes to ensure that the Standards are up to date with emerging threats and changes in the market.

PCI V3 CHANGE OVERVIEW

- **Network Diagrams**
 - Depicting the flow of cardholder data
- **Maintaining an Inventory**
 - E.g. Configuration Management Database
- **Consideration for Other Authentication Mechanisms**
 - Physical security tokens, smart cards and certificates
- **Documentation**
 - Requirement 12 previously a “Catch All”.

PCI V3 CHANGES CONTINUED

- **Protection of POS Terminals**
 - Protected from tampering and/or substitution
- **Service Provider: Clear Demarcation of Responsibilities**
 - Maintain a list of the responsibilities fulfilled by their service providers.
- **Service providers with remote access to customer premises**
 - Must use a unique authentication credential (such as a password/phrase) for each customer., e.g. no generic accounts

PCI V3 CHANGES CONTINUED

- **SNMP V1 & V2**
 - Considered to be insecure.
 - Documentation and business justification for use
- **Malware & Commonly Affected Systems**
 - Perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software
 - Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless authorized

PCI V3 CHANGES CONTINUED

- **Implement a Methodology for Penetration Testing**
 - Is based on industry-accepted penetration testing approaches
 - Includes coverage for the entire CDE perimeter & critical systems
 - Includes testing from both inside and outside the network
 - Includes testing to validate any segmentation and scope-reduction controls
 - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- **New requirement for coding practices** to protect against broken authentication and session management.
- **New requirement** to implement a process to respond to any alerts generated by a change detection software.

PCI V3 CHANGES CONTINUED

- **Re-direct services now in scope**
 - New SAQ A-EP
 - 138 requirements
- **SAQ A-EP**
 - Developed to address requirements applicable to e-commerce merchants with a website that does not itself receive cardholder data but which does effect the security of the payment transaction and/or the page that accepts the consumers cardholder data.
 - SAQ A-EP merchants are e-commerce merchants who partially outsource their e-commerce payment channel to a PCI DSS validated third party and do not electronically store, process or transmit data on their systems or premises.

PCI V3.1 NOW IN EFFECT

- **April 15, 2015**
 - Version 3.1 effective immediately
 - Version 3.0 will be retired June 30, 2015
- **Highlights**
 - Removal of SSL and earlier versions of TLS as secure protocols
 - 29 Clarifications
 - 4 Evolving Requirements (SSL)
 - 4 Additional Guidance (SMS for end-user messaging)

ADDITIONAL INTERESTING REQUIREMENTS

- **Requirement 6.6 :** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:
 - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
 - Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.
- **Requirement 11.3.1:** Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

ADDITIONAL INTERESTING REQUIREMENTS

- **Requirement 11.3.2:** Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
- **Requirement 11.3.4:** If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

WHAT IS EMV?



- EMV = Europay, Mastercard and Visa
- EMV, is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions.
- “Chip and Pin” is not an accurate description for the US implementation. More like “Chip and Signature”
- Main purpose is to reduce fraud by de-valuing stolen credit card data for “card present” transactions.
- Expect major fraud shift towards Mail Order/Telephone Order (MOTO) or “card not present” transactions



EMV LIABILITY SHIFT



- Liability Shift begins October 1, 2015
- Following the deadline “card-present” fraud liability will shift to whoever is the least EMV-compliant party in a fraudulent transaction.
- Any parties not EMV-ready by October 2015 could face much higher costs in the event of a large data breach.
- Automated fuel dispensers (pay at the pump) will have until 2017 to make the shift to EMV. Until then, they will follow existing fraud liability rulings.



EMV CREDIT CARD



EMV CREDIT CARD PROCESSING



Q & A

PCI Questions?

kperry@utah.gov

