Point of Sale System Architecture and Security

Lucas Zaichkowsky

lucas@accessdata.com

Twitter: @LucasErratus

AccessData

whoami

- IT and InfoSec geek since mid-90s
- Evangelist and researcher
- Subject matter expert:
  - Electronic payment processing and PCI
  - Cyber espionage
  - Cybercrime
  - Enterprise IR

Durango, CO
Population: 17,557

Serious Texas Bar-B-Q POS breach, 2010

AccessData

DH The Durango Herald 08/31

www.durangoherald.com/article/20100831/NEWS01/70831998

Serious Texas suffers card fraud

Restaurant's software vendor hacked

By Shane Benjamin Herald staff writer

Article Last Updated: Tuesday, August 31, 2010 2:53pm

-A A+ Share Recommend 0

Several hundred customers at Serious Texas Bar-B-Q were subject to debit-card fraud or attempted fraud earlier this year in Durango, police said.

Customers who used debit cards during February and March at Serious Texas Bar-B-Q may have had their card information stolen as part of a nationwide cyber breach, said Sgt. Dan Shry, investigator with the Durango Police Department.

Only customers at the south location, 650 South Camino del Rio, were affected, Shry said. Credit-card numbers also may have been stolen, he said, but so far, police have received reports only of debit-card fraud.

"I can assume credit cards were getting defrauded, too, but the main part of our cases were debit cards from local banks," Shry said.

More than 270 of the stolen credit cards used for fraud nationally

Mama's Boy POS breach, 2011

AccessData

The Durango Herald 10/28

durangoherald.com/article/20111028/NEWS01/71028991

100s of credit cards hacked

Computer virus at Mama's Boy found in mid-Oct.

By Shane Benjamin Herald staff writer

Article Last Updated: Thursday, October 27, 2011 11:07pm

Keywords: Fraud,

-A A+ Share Recommend 0

The Durango Police Department is warning residents about a large-scale debit- and credit-card fraud that occurred last month and earlier this month at Mama's Boy Italian Ristorante.

All credit and debit cards used at the restaurant between early August and mid-October were sent to a computer hacker, said Joe Farmer, investigator with the Durango Police Department.

"All of these cards are at risk of being duplicated," he said.

The computer system at the restaurant, 2659 Main Ave., was hacked in early August and infected with a virus that sends financial information back to the hacker, Farmer said. The virus was discovered in mid-October, he said.

Open since the 80s
Closed 4 months later

Iron Horse web site breach, 2013

AccessData

The Durango Herald 02/14

www.durangoherald.com/article/20130214/NEWS01/13021980

Iron Horse bike race reports fraud

Police looking into cause of compromised credit cards

By Shane Benjamin Herald staff writer

Article Last Updated: Thursday, February 14, 2013 11:27pm

Keywords: Iron Horse Bicycle Classic, Fraud,

-A A+ Share Recommend 95

Numerous people who registered for the Iron Horse Bicycle Classic may be victims of credit-card fraud, race officials said Thursday.

At least 20 people reported fraudulent activity since Sunday, said Gaige Sippy, race director for the event. Many more have come forward since news of the fraud was made public.

Race officials are unsure how widespread the problem is. They first learned of a possible problem Sunday, then received two more reports Monday and 15 reports Wednesday, Sippy said.

- Related media
- Letter sent to registrants

2,500 web site registrations
Unsure how many cards stolen

Since the breach, they moved to a hosted checkout solution

How many small business breaches? Probably thousands

AccessData

- In 2010, I personally saw several dozen POS breaches
- 190+ POS breaches in 2013 Verizon DBIR
  - Verizon is 1 of 23 PCI Forensics Investigators
- Breached small businesses sometimes notify customers
  - Post a notice on the store window
- Small merchant breaches rarely make the news in larger cities
  - The media has “better” content (e.g. violent crime, celebrities)

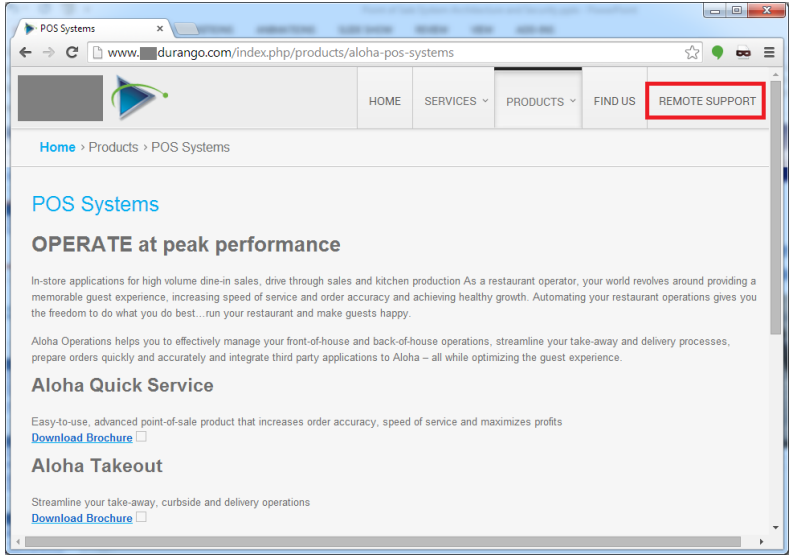
Small breaches are usually opportunistic

Opportunistic POS Attack Methodology:

1. Scan internet for pcAnywhere, VNC, RDP ports
2. Exploit vulnerable versions, brute force password guessing
3. Instant admin access to entire POS environment
4. Drop keystroke recorders, network sniffers, RAM scrapers
5. Automatically transmits stolen card data

Why so easy?!

- Small business owners use remote desktop to work remotely
  - “The POS dealer keeps me safe”
  - “Why would hackers come after me?”
- Local POS dealers use remote desktop for support
  - Most are power users
  - Security what?



Larger and More Sophisticated Incidents

Examples of targeted breach victims

- 2004 to 2006 - Boston Market, Barnes & Noble, Sports Authority, Forever 21
- 2005 - CardSystems, DSW, Office Max
- 2006 - TJX Companies, Inc.
- 2007 - Dave & Buster's
- 2008 - Hannaford, Heartland, RBS WorldPay
- 2011 - Sony, FIS
- 2012 - Global Payments
- 2013 - Target, Neiman Marcus
- 2014 - P.F. Chang's

Targeted breaches, legitimate hacking

Targeted Attack Methodology:

1. Perform footprinting and reconnaissance
2. Gain initial entry. Common methods…
   a) SQLi
   b) Buying backdoor access on black market
   c) Compromise a 3rd party with access
3. System and network enumeration
4. Privilege escalation
5. Lateral movement to establish a beachhead
   a) Drop a diverse set of backdoors
   b) Steal user passwords, target domain controllers and file servers
6. Find pivot points into the card data environment (CDE)
7. Modify code or drop malware to harvest card data
8. Exfiltrate undetected through obfuscation, throttled transfer rates, “blending in”

Fig. 1 “Hacker”

Windows isn't the problem

- They know Linux, Solaris, AIX, etc.
  - Backdoors are planted there too (e.g. LKMs)
  - Privileged credentials are stolen
- Systems for ATM limits and fraud detection are compromised
- Perform PIN-based attacks (e.g. HSM API brute force) [1]

[1] Webinar: "Don't be the next victim on PIN-Based attacks", Verizon Business 2009

Payment Processing Architecture Crash Course

Standalone terminals

- Dial-up and IP enabled
- Encrypted IP connection direct to processor
- Never(?) hacked remotely. Requires physical tampering

Electronic cash registers (ECRs)

- Communicate with each other on a hub using IRC (Inter-Register Communications)
- Communications device attached to one register connects over dial-up or encrypted IP direct to processor
- Never(?) hacked remotely. Requires physical tampering

Point of sale (POS)

- Most run on Windows
- POS terminals (aka registers) run the POS client component
- Registers communicate with a “back of house” POS server

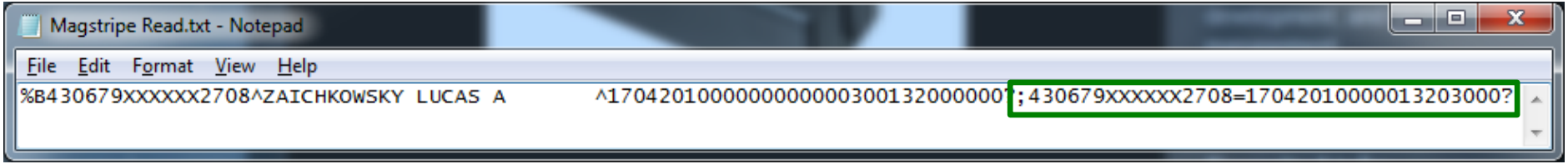
- Peripherals attach via USB or COM
  - Magstripe readers (MSR)
  - PIN Pads
  - PIN Pad/magstripe reader all-in-one
  - MICR check readers
  - Barcode scanners
  - Receipt printers

Magstripe Read Demo

Peripherals: Magstripe readers (MSRs)

- Most are configured for “keyboard emulation”
  - Swipe card > keyboard rapidly types magstripe data

- HID mode installs USB device with drivers and API interaction
- It’s all unencrypted
- Only Track2 is needed to clone magstripe cards for fraud



Peripherals: PIN pads

- Uses TDES algorithm and DUKPT key management for encrypting the PIN
  - Example encrypted PIN block: B07F65762F0F4701
  - Yes, this is secure
- Decryption keys are held by the payment processor, not the merchant
- PCI PIN Transaction Security (PTS) approved
  - Rigorous process with lots of anti-tampering requirements/testing

EMV Chip Read Demo

Peripherals: EMV readers

- Designed to reduce card-present fraud
  - Chip cannot be cloned
- EMV has “fallback mode” to support magstripe cards
  - When enabled, magstripe fraud is still a problem
- Chip contains magstripe “equivalent” data unencrypted
  - Different iCVV prevents use for magstripe fraud
  - Card number (PAN) and expiration date are unencrypted!
  - Card-not-present fraud still viable without CVV2

RAM dump during EMV chip read


```
236BB19AF9BAA069
3CF4F68C3386CD99
D1D........@...4
30679[redacted]2708.
=1704201000008360
3000?.9792CFFB3
9DE15661C386619.
17C1MÛ.....@...P
NS Interface - W
ait Response.360
3000F.Response>.
...<.B987A67B1F3
CF2....%...@...4
30679[redacted]2708=
1704201000008360
3000..A959336064
BA17BA75FD14AC46
821........@...A
0000000031010...
.nt1.7691825EED6
4E101CA.CF5C452A
1708B598996AD628
```

Magstripe Read.txt - Notepad

File Edit Format View Help

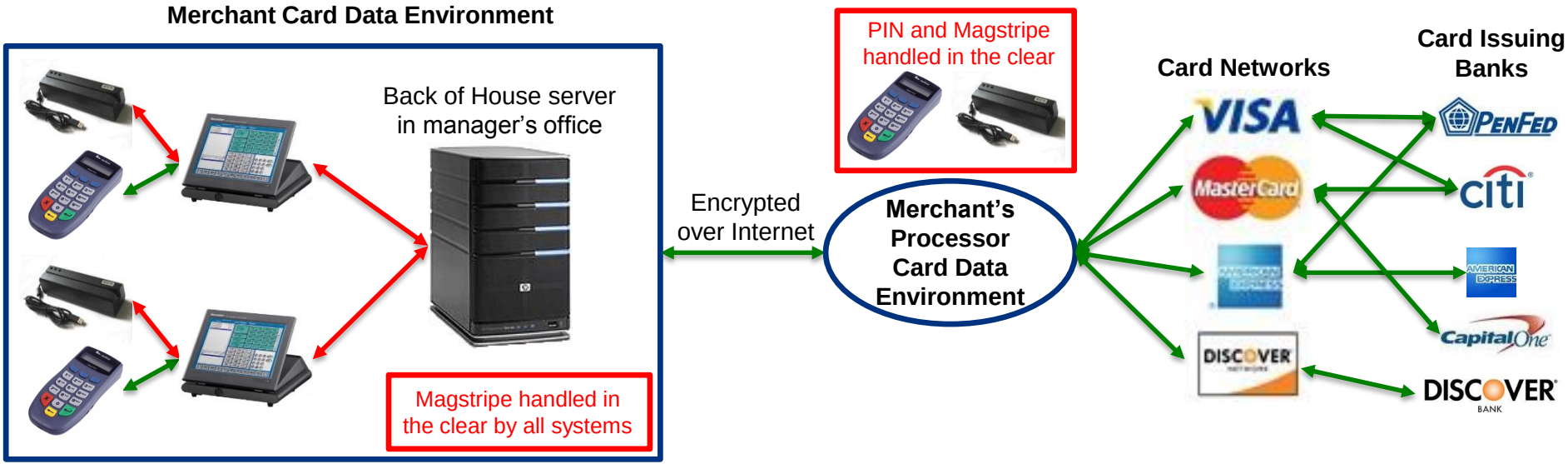
```
%B430679XXXXXX2708^ZAICHKOWSKY LUCAS A        ^17042010000000000003001320000000?;430679XXXXXX2708=170420100000132 03000?
```

Card Data Flow and Common Thieving Locations

Card data flow

- Card data environment (CDE) is **supposed** to be segmented from the rest of the network
- Encryption of sensitive card data is only required over untrusted networks

Encrypted **Unencrypted**



Card data flow: Service providers

- 3rd parties handle sensitive card data for the merchant
  - Web developers using shopping cart software
  - Online ordering services
  - Servers used by outsourced mobile applications
  - Value-add payment gateways

- Merchants by contract are supposed to hold 3rd parties liable
  - They rarely do
  - When a 3rd party service provider is breached, the merchant pays
  - Lawsuits!

Card data thievery

- POS terminals
  - Keystroke recorders, RAM scrapers
- POS back of house server
  - RAM scrapers, network sniffers, database theft
- Payment processors
  - RAM scrapers, network sniffers, database theft, HSM API brute force
- Web sites
  - Code modification, database theft

Practical Advice

Educate small business and POS dealers

- Stop using remote desktop software
  - Use a service like LogMeIn with two-factor auth enabled
    - LogMeIn supports one time PIN (OTP) via email for second factor
    - Use SMS email address so it only goes to a phone (e.g. 5551234567@vtext.com)
- Enable egress filtering, don't use POS systems for web/email
- Point to Point Encryption (P2PE)
  - When upgrading POS hardware, use encrypting peripherals
    - Software P2PE solutions are snake oil
  - Decryption should be done at the merchant's processor
  - Make sure keyed in card data and EMV are also encrypted

MagTek DynaPro

Larger targets

- Point to Point Encryption (P2PE)
- Know your network
- Know your enemy's TTPs (aka Intelligence-driven defense)
  - Don't underestimate their skills
- Spend more energy detecting and investigating incidents
  - A seemingly innocent alert could lead you to something major (e.g. psexec)
- Get executive support to harden systems and revoke local admin rights
  - Attackers steal and abuse privileged credentials
  - Protect and monitor their use accordingly

Questions?

Lucas Zaichkowsky

lucas@accessdata.com

Twitter: @LucasErratus