Data Breaches: The Secret Service Perspective

R. Matthew Chevraux
Assistant Special Agent in Charge
Office of Investigations
Cyber Strategy and Outreach
data breach
USSS – Integrated Mission

Physical Protection

Investigation of Financial Crimes
USSS History / Statutory Authority

1865 - Secret Service created to fight counterfeit currency

1901 - Assigned Presidential Protection duties

1948 - Title 18 USC § 470-474 (Counterfeiting & Forgery)

1984 - Title 18 USC § 1029-1030 (Access Device Fraud, Computer Hacking)

1986 - Title 18 USC § 1030 (Computer Hacking, Expanded)

1990 - Title 18 USC § 1344 (Bank Fraud)

1996 - Title 18 USC § 514 (Fictitious Obligations)

1998 - Title 18 USC § 1028 (Identity Theft, Expanded)

2001 - USA PATRIOT Act (Expanded Cyber Investigations & ECTFs)

2003 – Title 18 USC § 1037 (CAN-SPAM Act)

2004 - Title 18 USC § 1028A (Aggravated Identity Theft)
Electronic Crimes Task Forces (ECTFs)

- Electronic Crimes Task Forces – 40 Worldwide
- Trusted Partnerships Between Law Enforcement, Private Sector & Academia
- 4,000 Private Sector Partners
- 2,500 Federal, State, & Local Law Enforcement Partners
- 350 Academic Partners
- Coordinated Investigations, Information Sharing, Technical Expertise, and Training
Electronic Crimes Task Force: Principles for Success

- Respond quickly to cyber crimes incidents by coordinating people and equipment assets.
- Liaison with our trusted partners through quarterly meetings and other means of real time information sharing.
- Emphasize prevention for both our protective and investigative missions through preparation, education and training.
Priorities

Core Violations: Title 18, USC 1029 and 1030

• High dollar loss/community impact
• Organized groups/multi-defendant
• Transnational and multi-district investigations
• Identify new technology and schemes
Electronic Crimes Task Forces

United States Secret Service
Electronic Crimes Task Force
Field Locations
Who Is Being Targeted? 

- HBO
- Equifax Data Breach
- Target
- United States Office of Personnel Management
- The UPS Store
- Yahoo!
- Ashley Madison
- Sony Pictures
- Experian
- T-Mobile
- JPMorgan Chase
- The Home Depot Data Breach
<table>
<thead>
<tr>
<th>Motivations</th>
<th>Threats</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HACKTIVISM</strong></td>
<td>Hacktivists use computer network exploitation to advance their political or social causes.</td>
<td></td>
</tr>
<tr>
<td><strong>CRIME</strong></td>
<td>Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.</td>
<td></td>
</tr>
<tr>
<td><strong>INSIDER</strong></td>
<td>Trusted insiders steal proprietary information for personal, financial, and ideological reasons.</td>
<td></td>
</tr>
<tr>
<td><strong>ESPIONAGE</strong></td>
<td>Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.</td>
<td></td>
</tr>
<tr>
<td><strong>TERRORISM</strong></td>
<td>Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.</td>
<td></td>
</tr>
<tr>
<td><strong>WARFARE</strong></td>
<td>Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.</td>
<td></td>
</tr>
</tbody>
</table>
Describing the Incidents

2017 Data Breach Investigations Report
10th Edition
Who Are The Victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

Source: 2017 Verizon Data Breach Investigations Report
## What Else Is Common?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>66%</td>
<td>Of malware was installed via malicious email attachments.</td>
</tr>
<tr>
<td>73%</td>
<td>Of breaches were financially motivated.</td>
</tr>
<tr>
<td>21%</td>
<td>Of breaches were related to espionage.</td>
</tr>
<tr>
<td>27%</td>
<td>Of breaches were discovered by third parties.</td>
</tr>
</tbody>
</table>

*Source: 2017 Verizon Data Breach Investigations Report*
“Today’s Bank Robbers”

Question:
“Why do you rob banks?”

Answer:
“Because that’s where the money is.”

William “Slick Willie” Sutton
(Robbed over 100 banks from 1920 – 1952)

Information: PII, PHI, Credit Card & Financial Data, Intellectual Property
Simply stated, everyone is a target.
Large Scale Data Breaches

40 Million Credit Card Numbers Hacked

Data Breached at Processing Center

By Jonathan Krim and Michael S. D. Washington Post Staff Writers
Saturday, June 14, 2003; A01

More than 40 million credit cards used for fraud, MasterCard said.

In the largest security breach bearing the MasterCard logo, MasterCard said.

The breach occurred late last week.

The company said it is possible that the hack was a direct result of a more powerful and sophisticated attack.

Retailer TJX says 45 million card numbers stolen

NEW YORK (Reuters) - Off-price retailer TJX Cos said that information from about 45.7 million credit card accounts was stolen from its system.

The breach, which occurred sometime between late March and early April, affects customers of all the stores owned by the company, including Marshalls, T.J. Maxx, HomeGoods, Filene's Basement, andOperand.

The company said that it is working with law enforcement agencies to investigate the breach.

Heartland data breach could be bigger than TJX's

This recent incident suggests cybercriminals have shifted to targeting payment processors.

Jaikumar Vijayan

January 20, 2009 (Computerworld) A data breach disclosed today by Heartland Payment Systems Inc. may well displace TJX Companies Inc.'s January 2007 breach in the record books as the largest ever involving payment data with potentially over 100 million cards being compromised.

Heartland, a Princeton, N.J.-based provider of credit and debit card processing services, said that unknown intruders had broken into its systems sometime last year and planted malicious software to steal card data carried on the company's networks.

Visa and MasterCard alerted Heartland of suspicious activity, triggering the company to hold an investigation by "forensic investigators," during which the intrusion was discovered, Robert Baldwin Jr., Heartland's president and chief financial officer, said in a statement. The company said the intrusion may have been in the result of a "widespread global cyberfraud operation."
Who’s Behind the Breaches?

Source: 2017 Verizon Data Breach Investigations Report

- 75% perpetrated by outsiders.
- 25% involved internal actors.
- 18% conducted by state-affiliated actors.
- 3% featured multiple parties.
- 2% involved partners.
- 51% involved organized criminal groups.
The Threat – Transnational Organized Criminals

A group of Russian speaking, non-state actors have grown into a stable cartel and have technical, organizational and infrastructure capabilities of major concern to Homeland Security.
Overview – The Adversary

• Professional Criminal Organizations Pose Significant Threat To Networked Infrastructure Globally
  ▪ World-class technical skills
  ▪ Flush with funding and resources
  ▪ Access to transnational support infrastructure
• Most Serious Threats Operate From Abroad
  ▪ Well-organized groups building operations over the course of years
  ▪ Lax, ineffective or corrupt law enforcement regimes in home countries
  ▪ Some cybercrime hot spots relatively hostile to U.S. interests
• Criminal Threat Continues To Grow In Scope And Scale
Today’s Top Tier Cyber Criminal

- Capabilities That Exceed Most Nation States
  - Seemingly, unlimited funding & resources
- Expertise In Stealing Data
  - At rest, in-transit, encrypted
- Professional Relationships
  - Business-like organization
  - Trust / Reputation is everything
  - Code - Common beliefs for success
  - Money laundering networks
  - Profit-sharing
Today’s Top Tier Cyber Criminal (cont.)

- **Operational Security**
  - Russian speaking, no English allowed
  - "Need to Know" information sharing
  - Private communication networks
  - In-person meetings
  - Sophisticated encryption and obfuscation methods

- **Evolving Infrastructure**
  - Reinvestment to expand capabilities
  - Bulletproof hosting
  - Money laundering networks
  - Political power aspirations
Criminals Coordinate Through Carding Forums

- Carders often meet to discuss cybercrime, advertise their services and form conspiracies on websites known as “carding forums.”

- There are numerous carding forums each with many members. Members on carding forums register for accounts using nicknames (“nic”). These nics often become a cybercriminal’s brand and facilitate their activities.

- **Transactional Sites** (People Doing Business)
  - Stolen Credit Card Data
  - Stolen Databases of Personal Information
  - Online Banking
  - Online Payment Systems
  - Online Credit Card Processors
  - Counterfeit Identity Documents

- **Criminal Infrastructure Provision**
  - Hacking Services / Custom Malware Development
  - Phishing Services
  - Specialized Equipment (Card Writers, Embossers, Blank Credit Cards, Holograms, etc.)
  - Reshipping Services
  - Credit Reports and Personal Info Services
  - Bulletproof Hosting/Bot Net Services

- **Knowledge Sharing**
  - Technical Vulnerabilities
  - Sensitive Info on How Financial System Works
  - How to Defeat Security and Anti-Fraud Measures

- **Recruitment**
  - Finding Partners for Complex Fraud Schemes
ЗДРАВСТВУЙТЕ. ВЫ ЗАШЛИ НА САЙТ WWW.CARDERPLANET.COM

На нашем сайте обсуждаются уязвимости как онлайнов, так и офлайнов банковских продуктов, что, несомненно, будет полезно банковским специалистам для "заплатки" обсуждаемых "дыр". Наш сайт был открыт 31 мая 2001 года и за короткое время занял достойное место в группе сайтов посвященных вопросам электронной коммерции и банковской деятельности. Сайт CarderPlanet имеет своих мемберов, которые делятся по группам согласно их авторитету в той области области, на которой они специализируются. Мы рекомендуем Вам посетить наш форум и узнать мнение полезного. Все коммерческие объявления на сайте и на форуме платные. Если Вы разместите свое рекламное объявление коммерческого характера, предварительно не оплатив его, Ваше объявление будет удалено, а сами Вы будете заблокированы на нашем сайте. Мы рекомендуем Вам работать только с проверенными мемберами нашего сайта - в этом случае Вас не постигнет разочарование.

ФАЙЛОВЫЙ АРХИВ
Здесь вы можете скачать самые полезные программы и инструменты, которые пригодятся не только профессионалам, но и новичкам.

MEMBERS AREA
Username: [Blank]
Password: [Blank]

JOIN THE POWER!
Быть кардером, не просто кардером в Кардерон (с большой буквы) не так просто, но это даже не призыв - это судьба. Хочешь стать одним из нас?
Dumps Update USA & World

Base name: Ronald Reagan
Valid rate of firing: 100%
No Replacements!

Western Union transfers will be received in the next 48-72 hours! Money Gram transfers will be received 10-11 of June. Please note: 12, 13, 14, 15 of June are the government holidays in the drops country and Money Gram transfers will be received starting Monday June 16th. This does NOT affect Western Union transfers.

Credit Card Selection Update!

Base name: Machaon
Replacement time: 2 hours
Get yours while they last!
What Tactics They Use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Source: 2017 Verizon Data Breach Investigations Report
Confessions Of A “Top Tier” Russian Hacker

• Responsible for over $300 million in losses in some of the largest global data breaches
• Operated in the Russian Carding Forums
• 8+ year USSS investigation
• Apprehended and extradited to the United States with the aid of our international partners
Introvert – “lone wolf” with close circle of friends

No social media accounts

Learned to code early, learned SQL injections at university

Initial Motivation: Curiosity

Later on a “noble” purpose: By bringing attention to a problem, security becomes stronger

Believes “light drugs” can open the mind to creativity

Experienced “highs” from the thrill of gaining access to a network (became an addiction).
Wake up & “Get to work”
Read the news – traditional headlines, cyber & hacking forums
Work on 5 -6 “projects” at a time
  “Like being in a new city”
Get in and figure out network architecture better than IT Admin.
  “It’s like a puzzle. Gather enough pieces and the puzzle picture starts to appear. Soon you can imagine the whole network in your mind.”
NEVER work on “Russian Institution” project/Criminal Organization
Anatomy of a “Hack”

**RECON:**
- Often used google “site: yoursite.com + .asp”
- Returns all pages on a webserver
- Find an unpublished page ripe for SQL injection
- Port scans to determine servers and service
- Check firewall settings
INITIAL COMPROMISE:

- Webserver SQL Injection (almost always used)
- Spear phishing
- Botnet already on your network (cost $100-$1000)
- Insider (ex. Paid an employee to launch malware)
- Router attack
**Anatomy of a “Hack”**

**MAINTAIN PRESENCE:**

- Continually work to “clean up” systems to erase signs of compromise
- Multiple backdoors installed over time for persistence (.asp, .jsp)

He owned one company from 2000-2010
Top Tier Hacker’s Advice for IT Admin

- “You will never be able to build bulletproof system. Early detection is key.”
- Why best practices fail: “I can’t answer this question. Very simple rules. Maybe, human nature or laziness.” (Red Team verifies best practices)
  - Establish a BASELINE, you’ll need it to find what I’ve done (Snapshots)
  - Review Your Logs! (IDS does no good unless someone is monitoring)
  - How do you detect new devices on the network?
  - If you “Whitelist” applications, do you monitor this list to ensure no changes?
  - Flag geo lookup sites in your web logs (IP location search software)
  - Review net flow data (HBO, Sony)
  - Firewall Rules: “Will your firewall prevent me from reverse SSH’ing to my server?”
  - Complex & unique passwords (Where are they stored?)
Roman Valerevich Seleznev
aka “TRACK2”
Roman Seleznev was one of the world’s largest traffickers in stolen credit cards.

Seleznev was the protégé of one of the first cybercriminals who sold payment cards through a website (also previously arrested by USSS).

Installed malware on point of sale systems to steal credit card data.

Seleznev is a Russian national and previous attempts to arrest him were unsuccessful.

Seleznev has multiple Russian residences and periodically traveled to a home he maintained in Bali, Indonesia.
Seleznev’s Russian Political Ties

- Seleznev has made considerable wealth from his criminal activity and is politically connected.
- Roman Seleznev’s father is Valeriy S. Seleznev, a deputy in the Russian Duma (parliament), the representative from the Vladivostok region and a member of the ultra-nationalist Liberal Democratic Party of Russia.

Above: Russian MP Valeriy Seleznev’s website
Left: His son Roman Seleznev, the cybercriminal.
**Seleznev Judicial Action**

- July 5, 2014: Seleznev was successfully apprehended by USSS agents and arraigned in Guam. *1.7 million credit card #’s on seized laptop*
- August 2014: Extradited to Seattle, WA to stand trial
- August 25, 2016: Found guilty on 38 out of 40 counts, including Aggravated Identity Theft, Access Device Fraud, Hacking (18 USC 1030) and Wire Fraud
- April 21, 2017: Sentenced to 27 years
Selznev’s Impact

- Ran a vast credit card and identity theft operation responsible for over 400 intrusions
- Victims included 3,700 financial institutions, 500 global businesses
- Theft and resale of over 2 million credit card numbers
- $170 million in fraud loss
  - Received the longest sentence handed down in the United States for “hacking” charges
  - Highlights 10-year successful international, multi-agency cooperation
Universal Cyber Best Practices

- Update, patch, use current software (ex. Equifax)
- Routine password changes/complexity considerations (hardware too!)
- Multi-factor authentication
- Segmented networks
- Utilize practice of “least privilege”
- Encryption-Make the data unusable
- Net flow monitoring/baselining
- Use backups with integrity checks
- Routine employee cyber training
- Test your systems (Pen-Testing)/Employees (spear phishing)
What To Do – Before A Cyber Incident

• Have an cyber incident response plan!
  ▪ The adversary is planning for an attack, you should have a plan to recover/survive it!
• Have law enforcement contacts established already
• Have all sections participate in the development of your incident response plan.
  ▪ IT/Operations/Legal/C-Suite/Public Affairs/Law Enforcement(?)
• Review, test and exercise your incident response plan routinely and revise accordingly.
• If a breach occurs, coordinate with law enforcement early.
Understand that the adversary may still be monitoring your system.

• Consider going “out of band” with your mitigation communications
• Avoid actions that may alert the intruder (destructive malware?)
• Review your administrator accounts
• Consider restoring from backups (Are they compromised?)
• Messaging to your employees/Control the information
Calling Law Enforcement – What To Expect

• Contact the USSS as soon as possible
• Mitigate but don’t delete the evidence
• Keep malware and notate everything
• Maintain log files (at least 1 year)
• Theorize about what has happened
• Make your representatives available
• Mitigation and criminal investigation is a collaboration
• Going public is your decision - Your anonymity is preserved
• Bringing those responsible to justice may take time, patience
What Executive Leadership Needs to Know

1. Partnership is a benefit
   - LE is not a regulator, meet & know your LE partners – Before!

2. Information sharing is knowledge sharing
   - Discuss priorities and where LE can provide knowledge

3. Know where risk exists in your IT systems
   - No unlimited funds, have a plan and consider insider threats

4. Know their role in the company’s incident response plan
   - Exercise your Cyber IRP and know what your people will require

5. Know what you’re going to do when law enforcement calls
   - Help the C-Suite/Legal with basic cyber literacy and what law enforcement will need
The Future?

What will the Warrior-Guardian of the future look like?

Yo! Dude... Back here.