

CUTTING OFF THE HYDRA HEADS OF ACH WIRE FRAUD

Presented by:

Eigen Heald, MsIA, CISA, CISSP, CGEIT, CEH, GCFA

Agenda

- Introductions
- Definitions
- Current Statistics
- Causes
- Risks
- A Case Study
- Wire Fraud Explained
- Nine Solutions
- Questions and Answers

Introductions

Introductions



Eigen Heald, MsIA

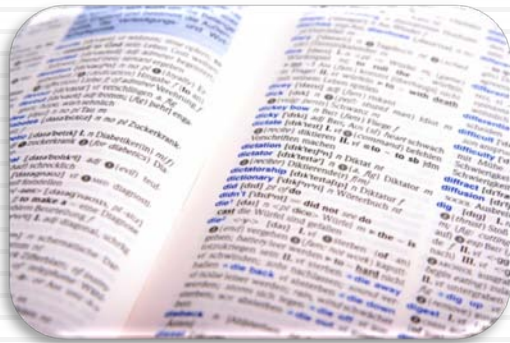
- IT security professional and Consulting Manager at Berry, Dunn, McNeil & Parker
- Industry certifications include:
 - Certified Information Systems Auditor
 - Certified Information Systems Security Professional
 - Certified Ethical Hacker
 - Certified in the Governance of Enterprise IT
 - GIAC Certified Forensic Analyst

The Issue:

According to the FBI, in 2008-2009 there has been a "significant increase" in fraud involving the exploitation of *valid online banking credentials* belonging to:

- Colleges and universities
- Non-profit organizations
- Municipal government
- Small and medium businesses

Definitions



Key terms we will discuss during this presentation

Definitions

Automated Clearing House (ACH)

- Electronic network for financial transactions
- Processes direct deposit payroll, vendor payments, consumer payments, transfers to/from financial institutions, etc.

Electronic Fund Transfers

- Used to transfer funds to another bank account (usually set up by a “money mule”) where it is drawn out or sent overseas

Definitions

“Trojan Horse” Software

- Software code that facilitates unauthorized access to the user's computer system
- Can “call home” to request code that specifically targets the user, then installs the code in the background

“Money Mule”

- Individuals (often hired by the criminals) set up bank accounts, withdraw the fraudulent transfers, and wire the money out of the country
- Most frequently the money is wired to countries in Eastern Europe

Definitions

“Malware”

- Computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet

“Spear Phishing”

- *Targeted* emails directed to employees most likely to have access to bank account information (e.g., CFO, CEO, COO, Senior Auditor)

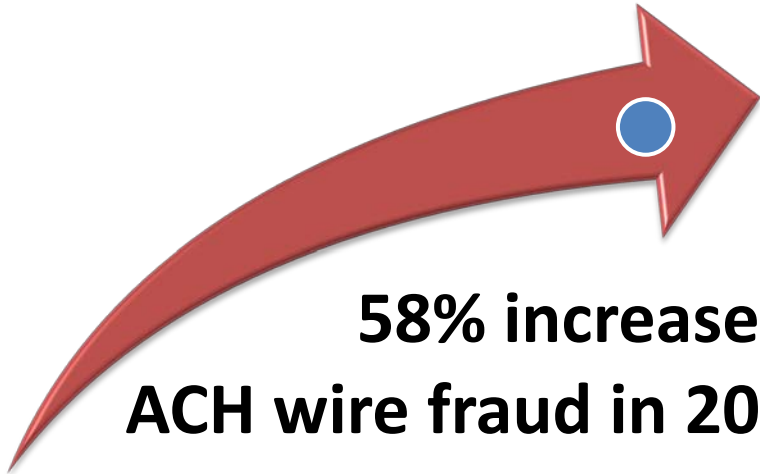
Current Statistics



How ACH wire fraud affects different groups

2008 Statistics

- According to the Financial Crimes Enforcement Network (a Treasury Department division):

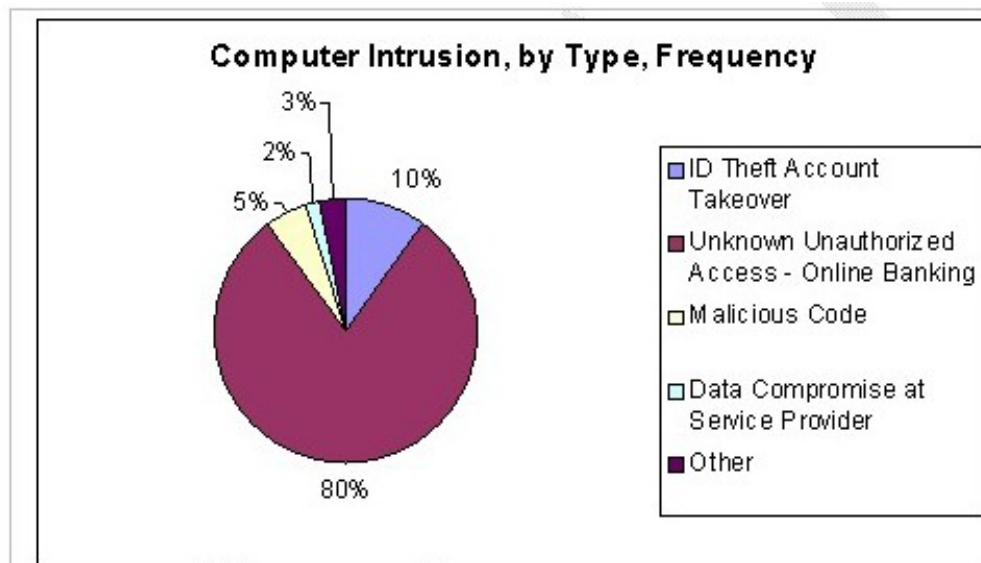


**58% increase in
ACH wire fraud in 2008**

- Reliable figures about losses from online banking fraud are difficult to come by and many incidents go unreported

2009 Statistics

- As of November 2009, losses of \$40 million attributed to ACH wire fraud
- Over \$85 million in attempts



Identifying the cause of the computer intrusion is often not possible, since often the intrusion originated from the customers PC. Several [case studies](#) are included that describe this scenario.

90 Percent Confidence Interval: ID Theft Account Takeover = 10.0% ± 6.4%;
Trojan Horse/Spyware (Malicious Code): 90% confidence interval = 5.2% ± 4.6%

Sample Statistics: Education

- [MARIAN COLLEGE](#) August 5, 2009
\$189,000 (Regained: \$0)
- [SAND SPRINGS SCHOOLS](#) August 12, 2009
\$150,000 (Regained: \$70,000)
- [SANFORD SCHOOL DISTRICT](#) August 19, 2009
\$117,000 (Regained: \$99,000)
- [SYCAMORE COUNTY SCHOOLS](#) July 9, 2009
\$300,000 (Regained: \$0)

Sample Statistics: Non-Profits

- [EVERGREEN CHILDREN'S ASSN](#) September 9, 2009
\$30,000 (Regained: \$30,000)
- [STEUBEN ARC](#) September 22, 2009
\$200,000 (Regained: \$42,000)
- [UNITED METHODIST CHURCH](#) September 30, 2009
\$33,300 (Regained: \$0)
- [ST. ISIDORE'S CATHOLIC CHURCH](#) September 30, 2009
\$87,000 (Regained: \$0)

Causes



Common causes of
ACH wire fraud

Causes

- Small and medium-sized colleges and universities have fewer IT resources
- Tendency to believe that because of size, the educational institution won't be vulnerable
- “Open campus” model
- Tendency to “set it and forget it”
- Fewer personnel to monitor daily banking activity

Risks



Risks associated with
ACH wire fraud

Risks

- Loss of reputation
- Regulatory penalties
- Financial loss due to bank controls for commercial accounts

Commercial Accounts, Less Protection

- *Consumers* typically have up to 60 days from the receipt of a monthly statement to dispute any unauthorized charges
- Commercial banking customers have roughly **two business days** to spot and dispute unauthorized activity if they want to hold out any hope of recovering unauthorized transfers from their accounts
- Thieves tend to wire out multiple transactions below \$10,000 to avoid scrutiny

A Case Study

How does it happen?



Wire fraud explained

A Common Attack

- Targeted emails (“spear phishing”) can install custom code via PDF or other documents
- “Drive-by” installation from web pages (e.g., Internet-based custom code written by cybercriminals from various parts of the world)
- Custom code specifically looks for banking information inside the web browser
- Code captures user ID, password, even bank “pictures” used for two-factor authentication

“Drive By” Code Installation

- Malicious code is no longer limited to porn and other sleazy websites
- Hackers are targeting more commonly used higher education, healthcare, blogging, and small eCommerce websites
- Last August (2009), over 60,000 websites were infected by *one* exploit

Nine Solutions



Minimizing your risk of
ACH wire fraud

Nine Solutions

1. Stop conducting ACH wire transfers over the Internet
 - Does not eliminate Internet banking risk
2. Stop conducting Internet banking
 - Not always feasible
3. Develop specific control procedures with the bank
 - Bank will not always agree (but many will)

Nine Solutions

4. Increase IT staffing so more security activity can be implemented and maintained
 - Activity may still be missed
5. Run the best anti-virus software and update daily
 - May not catch latest malware
6. Monitor outbound connections
 - Will catch connections to unusual locations, but won't catch malware if it is routed within normal IP addressing range

Nine Solutions

7. Acquire two-factor authentication from the bank
 - Requires a token
8. Utilize a separate PC to conduct online banking and nothing else
 - Recommended by the ABA and FBI
 - Requires a separate PC

Nine Solutions

9. Utilize a virtual machine desktop that will load a virtual operating system inside a single PC
 - Virtual operating system can be turned on for Internet banking and then closed
 - Requires a more powerful single PC

Questions?

Eigen Heald, Consulting Manager

Berry, Dunn, McNeil & Parker

Phone: (207) 541-2311

ehald@bdmp.com

BERRY. DUNN. MCNEIL & PARKER

